EXHIBIT 14

As filed with the U.S. Securities and Exchange Commission on September 22, 2021.

Registration No. 333-

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549

FORM S-1
REGISTRATION STATEMENT
UNDER
THE SECURITIES ACT OF 1933

IronNet, Inc.

(Exact name of registrant as specified in its charter)

Delaware	7372	83-4599446
(State or other jurisdiction of incorporation or organization)	(Primary Standard Industrial Classification Code Number)	(I.R.S. Employer Identification No.)

7900 Tysons One Place, Suite 400
McLean, VA
(443) 300-6761
(Address, including zip code, and telephone number, including area code, of registrant's principal executive offices)

Scott Alridge
Chief Legal Officer and Secretary
IronNet, Inc.
7900 Tysons One Place, Suite 400
McLean, VA 22102
(201) 793-1111
(Name, address, including zip code, and telephone number, including area code, of agent for service)

Copies to:

Brian F. Leaf
Garth A. Osterman
Cooley LLP
One Freedom Square
Reston Town Center
11951 Freedom Drive
Reston, VA 20190
(703) 456-8000

Approximate date of commencement of proposed sale to the public: As soon as practicable after this Registration Statement is declared effective.

If any of the securities being registered on this Form are to be offered on a delayed or continuous basis pursuant to Rule 415 under the Securities Act of 1933, check the following box. ☒

If this Form is filed to register additional securities for an offering pursuant to Rule 462(b) under the Securities Act, please check the following box and list the Securities Act registration statement number of the earlier effective registration statement for the same offering. ☐

If this Form is a post-effective amendment filed pursuant to Rule 462(c) under the Securities Act, check the following box and list the Securities Act registration statement number of the earlier effective registration statement for the same offering. ☐

If this Form is a post-effective amendment filed pursuant to Rule 462(d) under the Securities Act, check the following box and list the Securities Act registration statement number of the earlier effective registration statement for the same offering. ☐

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer, smaller reporting company, or an emerging growth company. See the definitions of "large accelerated filer," "accelerated filer," "smaller reporting company," and "emerging growth company" in Rule 12b-2 of the Exchange Act.

Large accelerated filer	☐	Accelerated filer	☐
Non-accelerated filer	☒	Smaller reporting company	☒
		Emerging growth company	☒

If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 7(a)(2)(B) of the Securities Act. ☐

CALCULATION OF REGISTRATION FEE

Title of Each Class of Securities To Be Registered	Amount to be Registered(1)	Proposed Maximum Aggregate Offering Price Per Security	Proposed Maximum Aggregate Offering Price	Amount of Registration Fee
Primary Offering				
Common stock, $0.0001 par value per share	13,824,992 (2)	$28.59 (5)	$395,256,521.28	$43,122.49 (5)
Secondary Offering				
Common stock, $0.0001 par value per share	64,020,756 (3)	$28.59 (5)	$1,830,353,414.04	$199,691.56 (5)
Warrants to purchase common stock	5,200,000 (4)	—	—	— (6)
Total common stock	77,845,748	$28.59	$2,225,609,935.32	$242,814.05

(1) In the event of a stock split, stock dividend or other similar transaction involving the registrant's common stock, in order to prevent dilution, the number of shares of common stock registered hereby shall be automatically increased to cover the additional shares of common stock in accordance with Rule 416(a) under the Securities Act.

(2) Consists of (i) 5,200,000 shares of common stock issuable upon the exercise of 5,200,000 warrants issued to LGL Systems Acquisition Holding Company, LLC (the "**Sponsor**") in a private placement (the "**Private Warrants**") and (ii) 8,624,992 shares of common stock issuable upon the exercise of 8,624,992 warrants included in the publicly sold units (the "**Public Warrants**") to purchase common stock, in each case at an exercise price of $11.50 per share.

(3) Consists of (i) 2,904,375 shares of common stock that were exchanged for the Class B common stock, par value $0.0001 per share ("**LGL Class B Common Stock**"), (ii) 12,500,000 shares of common stock issued pursuant to subscription agreements entered into on March 15, 2021, (iii) up to 5,200,000 shares of common stock that may be issued upon exercise of the Private Warrants and (iv) 43,416,381 shares of common stock (including up to 81,412 shares of common stock issuable pursuant to outstanding options, 7,465,923 shares of common stock issuable in connection with the vesting and settlement of restricted stock units, and 560,703 shares of common stock that were issued as Earnout Shares (as defined below) on September 17, 2021) pursuant to that certain Amended and Restated Registration Rights Agreement, dated August 26, 2021, between us and the selling securityholders granting such holders registration rights with respect to such shares.

(4) Represents the resale of 5,200,000 Private Warrants.

(5) Estimated solely for the purpose of calculating the registration fee in accordance with Rule 457(c) under the Securities Act. The price per share and aggregate offering price are based on the average of the high and low prices of the Registrant's common stock on September 15, 2021, as reported on the New York Stock Exchange.

(6) In accordance with Rule 457(i), the entire registration fee for the Private Warrants is allocated to the shares of common stock underlying the Private Warrants, and no separate fee is payable for the Private Warrants.

The Registrant hereby amends this Registration Statement on such date or dates as may be necessary to delay its effective date until the Registrant shall file a further amendment which specifically states that this Registration Statement shall thereafter become effective in accordance with Section 8(a) of the Securities Act of 1933 or until the Registration Statement shall become effective on such date as the Commission, acting pursuant to said Section 8(a), may determine.

The information in this preliminary prospectus is not complete and may be changed. These securities may not be sold until the registration statement filed with the Securities and Exchange Commission is effective. This preliminary prospectus is not an offer to sell these securities nor does it seek an offer to buy these securities in any jurisdiction where the offer or sale is not permitted.

Subject to Completion, Dated September 22, 2021

PRELIMINARY PROSPECTUS

Up to 64,020,756 Shares of Common Stock
Up to 13,824,992 Shares of Common Stock Issuable Upon Exercise of Warrants
Up to 5,200,000 Warrants to Purchase Common Stock

This prospectus relates to the issuance by us of an aggregate of up to 13,824,992 shares of our common stock, $0.0001 par value per share (the "**common stock**"), which consists of (i) up to 5,200,000 shares of common stock that are issuable upon the exercise of 5,200,000 warrants (the "**Private Warrants**") originally issued in a private placement to LGL Systems Acquisition Holding Company, LLC (the "**Sponsor**") in connection with the initial public offering of LGL Systems Acquisition Corp. ("**LGL**") and (ii) up to 8,624,992 shares of common stock that are issuable upon the exercise of 8,624,992 warrants (the "**Public Warrants**" and, together with the Private Warrants, the "**Warrants**") originally issued in the initial public offering of LGL. We will receive the proceeds from any exercise of any Warrants for cash.

This prospectus also relates to the offer and sale from time to time by the selling securityholders named in this prospectus or their permitted transferees (the "**selling securityholders**") of (i) up to 64,020,756 shares of common stock consisting of (a) up to 12,500,000 shares of common stock issued in a private placement pursuant to subscription agreements (the "**Subscription Agreements**") entered into on March 15, 2021, (b) up to 2,904,375 shares of common stock issued in a private placement to the Sponsor in connection with the initial public offering of LGL (the "**Founder Shares**"), (c) up to 5,200,000 shares of common stock issuable upon exercise of the Private Warrants and (d) up to 43,416,381 shares of common stock (including up to 81,412 shares of common stock issuable pursuant to outstanding options, 7,465,923 shares of common stock issuable in connection with the vesting and settlement of restricted stock units, and 560,703 shares of common stock that were issued as Earnout Shares (as defined below) on September 17, 2021) pursuant to that certain Amended and Restated Registration Rights Agreement, dated August 26, 2021, between us and the selling securityholders granting such holders registration rights with respect to such shares and (ii) up to 5,200,000 Private Warrants. We will not receive any proceeds from the sale of shares of common stock or Warrants by the selling securityholders pursuant to this prospectus.

The selling securityholders may offer, sell or distribute all or a portion of the securities hereby registered publicly or through private transactions at prevailing market prices or at negotiated prices. We will not receive any of the proceeds from such sales of the shares of common stock or Warrants, except with respect to amounts received by us upon exercise of the Warrants. We will bear all costs, expenses and fees in connection with the registration of these securities, including with regard to compliance with state securities or "blue sky" laws. The selling securityholders will bear all commissions and discounts, if any, attributable to their sale of shares of common stock or Warrants. See the section titled "*Plan of Distribution*."

Our common stock and Warrants are listed on the New York Stock Exchange under the symbols "IRNT" and "IRNT.WS", respectively. On September 20, 2021, the last reported sales price of our common stock was $33.34 per share and the last reported sales price of our Warrants was $7.88 per warrant.

We are an "emerging growth company" as defined under U.S. federal securities laws and, as such, have elected to comply with reduced public company reporting requirements. This prospectus complies with the requirements that apply to an issuer that is an emerging growth company.

Investing in our securities involves a high degree of risks. You should review carefully the risks and uncertainties described in the section titled "Risk Factors" beginning on page 7 of this prospectus, and under similar headings in any amendments or supplements to this prospectus.

Neither the Securities and Exchange Commission nor any state securities commission has approved or disapproved of these securities, or passed upon the accuracy or adequacy of this prospectus. Any representation to the contrary is a criminal offense.

Prospectus dated , 2021

ABOUT THIS PROSPECTUS

This prospectus is part of a registration statement on Form S-1 that we filed with the Securities and Exchange Commission (the "**SEC**") using the "shelf" registration process. Under this shelf registration process, the selling securityholders may, from time to time, sell the securities offered by them described in this prospectus. We will not receive any proceeds from the sale by such selling securityholders of the securities offered by them described in this prospectus. This prospectus also relates to the issuance by us of the shares of common stock issuable upon the exercise of any Warrants. We will not receive any proceeds from the sale of shares of common stock underlying the Warrants pursuant to this prospectus, except with respect to amounts received by us upon the exercise of the Warrants for cash.

Neither we nor the selling securityholders have authorized anyone to provide you with any information or to make any representations other than those contained in this prospectus or any applicable prospectus supplement or any free writing prospectuses prepared by or on behalf of us or to which we have referred you. Neither we nor the selling securityholders take responsibility for, and can provide no assurance as to the reliability of, any other information that others may give you. Neither we nor the selling securityholders will make an offer to sell these securities in any jurisdiction where the offer or sale is not permitted.

We may also provide a prospectus supplement or post-effective amendment to the registration statement to add information to, or update or change information contained in, this prospectus. You should read both this prospectus and any applicable prospectus supplement or post-effective amendment to the registration statement together with the additional information to which we refer you in the sections of this prospectus titled *"Where You Can Find More Information."*

On August 26, 2021, Legacy IronNet, LGL and Merger Sub (as such terms are defined below), consummated the closing of the transactions contemplated by the Business Combination Agreement (as defined below). Pursuant to the terms of the Business Combination Agreement, a business combination of Legacy IronNet and LGL was effected by the merger of Merger Sub with and into Legacy IronNet, with Legacy IronNet surviving the Business Combination (as defined below) as a wholly-owned subsidiary of LGL. Following the consummation of the Business Combination on the Closing Date (as defined below), LGL changed its name from LGL Systems Acquisition Corp. to IronNet, Inc.

Unless the context indicates otherwise, references in this prospectus to the "IronNet," "we," "us," "our" and similar terms refer to IronNet, Inc. (f/k/a LGL Systems Acquisition Corp.) and its consolidated subsidiaries (including Legacy IronNet). References to "LGL" refer to the predecessor company prior to the consummation of the Business Combination.

SPECIAL NOTE REGARDING FORWARD-LOOKING STATEMENTS

This prospectus contains "forward-looking statements" that involve substantial risks and uncertainties. The forward-looking statements are contained principally in the sections titled "Prospectus Summary" "Risk Factors," "Management's Discussion and Analysis of Financial Condition and Results of Operations," "Business" and elsewhere in this prospectus. In some cases, you can identify forward-looking statements by terms such as "anticipate," "believe," "continue," "could," "estimate," "expect," "intend," "may," "might," "objective," "ongoing," "plan," "potential," "predict," "project," "should," "will" and "would," or the negative of these terms or other similar expressions intended to identify statements about the future. These statements speak only as of the date of this prospectus and involve known and unknown risks, uncertainties and other important factors that may cause our actual results, performance or achievements to be materially different from any future results, performance or achievements expressed or implied by the forward-looking statements. We have based these forward-looking statements largely on our current expectations and projections about future events and financial trends that we believe may affect our business, financial condition and results of operations. These forward-looking statements include, without limitation, statements about:

- our ability to recognize the anticipated benefits of the Business Combination, which may be affected by, among other things, competition and the ability of the combined business to grow and manage growth profitably;
- costs related to the Business Combination;
- our future operating or financial results;
- future acquisitions, business strategy and expected capital spending;
- changes in our strategy, future operations, financial position, estimated revenues and losses, projected costs, prospects and plans;
- the implementation, market acceptance and success of our business model and growth strategy;
- our expectations and forecasts with respect to the size and growth of the cybersecurity industry and our products and services in particular;
- the ability of our products and services to meet customers' compliance and regulatory needs;
- our ability to compete with others in the cybersecurity industry;
- our ability to retain pricing power with our products;
- our ability to grow our market share;
- our ability to attract and retain qualified employees and management;
- our ability to adapt to changes in consumer preferences, perception and spending habits and develop and expand our product offerings and gain market acceptance of our products, including in new geographies;
- developments and projections relating to our competitors and industry;
- our ability to develop and maintain our brand and reputation;
- developments and projections relating to our competitors and industry;
- the impact of health epidemics, including the COVID-19 pandemic, on our business and on the economy in general;
- the impact of the COVID-19 pandemic on customer demands for our products;
- our expectations regarding our ability to obtain and maintain intellectual property protection and not infringe on the rights of others;

- expectations regarding the time during which we will be an emerging growth company under the JOBS Act;
- our future capital requirements and sources and uses of cash;
- our ability to obtain funding for our operations and future growth; and
- our business, expansion plans and opportunities.

The foregoing list of risks is not exhaustive. Other sections of this prospectus may include additional factors that could harm our business and financial performance. Moreover, we operate in an evolving environment. New risk factors and uncertainties may emerge from time to time, and it is not possible for management to predict all risk factors and uncertainties. As a result of these factors, we cannot assure you that the forward-looking statements in this prospectus will prove to be accurate. Except as required by applicable law, we do not plan to publicly update or revise any forward-looking statements contained herein, whether as a result of any new information, future events, changed circumstances or otherwise, except as required by law.

Because forward-looking statements are inherently subject to risks and uncertainties, some of which cannot be predicted or quantified and some of which are beyond our control, you should not rely on these forward-looking statements as predictions of future events. Although we believe that we have a reasonable basis for each forward-looking statement contained in this prospectus, the events and circumstances reflected in our forward-looking statements may not be achieved or occur and actual results could differ materially from those projected in the forward-looking statements. You should refer to the ‘‘Risk Factors’’ section of this prospectus for a discussion of important factors that may cause our actual results to differ materially from those expressed or implied by our forward-looking statements.

You should read this prospectus and the documents that we reference in this prospectus and have filed as exhibits to the registration statement, of which this prospectus is a part, completely and with the understanding that our actual future results may be materially different from what we expect. We qualify all of our forward-looking statements by these cautionary statements.

In addition, statements that “we believe” and similar statements reflect our beliefs and opinions on the relevant subject. These statements are based upon information available to us as of the date of this prospectus and while we believe such information forms a reasonable basis for such statements, such information may be limited or incomplete, and such statements should not be read to indicate that we have conducted an exhaustive inquiry into, or review of, all potentially available relevant information. These statements are inherently uncertain, and investors are cautioned not to unduly rely upon these statements.

TABLE OF CONTENTS

You should rely only on the information contained in this prospectus, any supplement to this prospectus or in any free writing prospectus, filed with the SEC. Neither we nor the selling securityholders have authorized anyone to provide you with additional information or information different from that contained in this prospectus filed with the SEC. We take no responsibility for, and can provide no assurance as to the reliability of, any other information that others may give you. The selling securityholders are offering to sell, and seeking offers to buy, our securities only in jurisdictions where offers and sales are permitted. The information contained in this prospectus is accurate only as of the date of this prospectus, regardless of the time of delivery of this prospectus or any sale of our securities. Our business, financial condition, results of operations and prospects may have changed since that date.

For investors outside of the United States: Neither we nor the selling securityholders, have done anything that would permit this offering or possession or distribution of this prospectus in any jurisdiction where action for that purpose is required, other than in the United States. Persons outside the United States who come into possession of this prospectus must inform themselves about, and observe any restrictions relating to, the offering of our securities and the distribution of this prospectus outside the United States.

RISK FACTORS

Investing in our common stock involves a high degree of risk. You should carefully consider the risks and uncertainties described below together with all of the other information contained in this prospectus, including our financial statements and related notes appearing at the end of this prospectus and in the section titled "Management's Discussion and Analysis of Financial Condition and Results of Operations," before deciding to invest in our common stock. If any of the events or developments described below were to occur, our business, prospects, operating results and financial condition could suffer materially, the trading price of our common stock could decline, and you could lose all or part of your investment. The risks and uncertainties described below are not the only ones we face. Additional risks and uncertainties not presently known to us or that we currently believe to be immaterial may also adversely affect our business.

Risks Related to Our Business and Industry

We have experienced rapid growth in recent periods, and if we do not manage our future growth, our business and results of operations will be adversely affected.

We have experienced rapid revenue growth in recent periods we expect to continue to invest broadly across our organization to support our growth. For example, our headcount grew from 196 full-time employees as of January 31, 2019 to 246 full-time employees as of January 31, 2021 and 296 full-time employees as of July 31, 2021. Although we have experienced rapid growth historically, we may not be able sustain our current growth rates, nor can we assure you that our investments to support our growth will be successful. The growth and expansion of our business will require us to invest significant financial and operational resources and the continuous dedication of our management team. We have encountered and will continue to encounter, risks and difficulties frequently experienced by rapidly growing companies in evolving industries, including market acceptance of our products, adding new customers, intense competition, and our ability to manage our costs and operating expenses. Our future success will depend in part on our ability to manage our growth effectively, which will require us to, among other things:

- effectively attract, integrate and retain a large number of new employees, particularly members of our sales and marketing, data science, and research and development teams;
- further improve our platform and products, including our cloud modules and security capabilities, analytics, collective defense capabilities, and visualizations, and IT infrastructure, including expanding and optimizing our data centers, collection, and analytic capabilities, to support our business needs;
- enhance our information and communication systems to ensure that our employees and offices around the world are well coordinated and can effectively communicate with each other and our growing base of customers and partners; and
- improve our financial, management, and compliance systems and controls.

If we fail to achieve these objectives effectively, our ability to manage our expected growth, ensure uninterrupted operation of our platform and key business systems, and comply with the rules and regulations applicable to our business could be impaired. Additionally, the quality of our platform and services could suffer and we may not be able to adequately address competitive challenges. Any of the foregoing could adversely affect our business, results of operations, and financial condition.

We have a history of losses and may not be able to achieve or sustain profitability in the future.

We have incurred net losses in all periods since our inception. We experienced net losses of $55.4 million and $47.9 million for fiscal 2021 and fiscal 2020, respectively, and $32.7 million and $30.7 million for the six months ended July 31, 2021 and 2020, respectively. As of July 31, 2021, we had an accumulated deficit of $207.7 million. While we have experienced significant growth in revenue in recent periods, we cannot predict

when or whether we will reach or maintain profitability. We also expect our operating expenses to increase over our historical expenses in the future as we continue to invest for future growth, which will negatively affect our results of operations if our total revenue does not increase. We cannot assure you that these investments will result in substantial increases in our total revenue or improvements in our results of operations. In addition to the anticipated costs to grow our business, we also expect to incur significant additional legal, accounting, and other expenses as a newly public operating company. Any failure to increase our revenue as we invest in our business or to manage our costs could prevent us from achieving or maintaining profitability or positive cash flow.

Our limited operating history makes it difficult to evaluate our current business and our future prospects and may increase the risk of your investment.

Legacy IronNet was founded in 2014 and we launched our first cybersecurity network detection and response product in 2016 (IronDefense) and our first collective defense product in 2018 (IronDome). Our limited operating history makes it difficult to evaluate our current business, our future prospects, and other trends, including our ability to plan for and model future growth. We have encountered, and we will continue to encounter, risks, uncertainties, and difficulties frequently experienced by rapidly growing companies in evolving industries, including our ability to achieve broad market acceptance of cloud- enabled, and/or software as a service ("**SaaS**") delivered cybersecurity solutions and our platform, attract additional customers, grow partnerships, compete effectively, build and maintain effective compliance programs, and manage increasing expenses as we continue to invest in our business. If we do not address these risks, uncertainties and difficulties successfully, our business, and results of operations will be harmed. Further, we have limited historical financial data and operate in a rapidly evolving market. As a result, any predictions about our future revenue and expenses may not be as accurate as they would be if we had a longer operating history or operated in a more predictable market.

The COVID-19 pandemic could adversely affect our business, operating results and future revenue.

In March 2020, the World Health Organization declared COVID-19 a global pandemic. This contagious disease outbreak has spread across the globe and is impacting worldwide economic activity and financial markets. In light of the uncertain and rapidly evolving situation relating to the spread of COVID-19, we have taken precautionary measures intended to mitigate the spread of the virus and minimize the risk to our employees, customers, partners, and the communities in which we operate. These measures include transitioning our employee population to work remotely from home, imposing travel restrictions for our employees, shifting customer, partner and investor events to virtual-only formats, and limiting capacity at any of our offices which have reopened or may reopen during the pandemic's duration. These precautionary measures, many of which we have now made largely permanent and sustainable, and associated economic issues, both in the United States and across the globe, could negatively affect our CS efforts, significantly delay and lengthen our sales cycles, impact our sales and marketing efforts, reduce employee efficiency and productivity, slow our international expansion efforts, increase cybersecurity risks, and create operational or other challenges, any of which could harm our business and results of operations. Moreover, due to our subscription-based business model, the effect of the COVID-19 pandemic may not be fully reflected in our results of operations until future periods, if at all.

In addition, the COVID-19 pandemic may disrupt the operations of our prospective clients, customers, and partners for an indefinite period of time. Some of our customers have been negatively impacted by the COVID-19 pandemic, which could result in delays in accounts receivable collection, or result in decreased technology spending, including spending on cybersecurity, which could negatively affect our revenues. Some of our prospective clients have also been negatively impacted by the COVID-19 pandemic, which could result in delays in sales or lengthen purchasing decisions.

More generally, the COVID-19 pandemic has adversely affected economies and financial markets globally, and continued uncertainty could lead to a prolonged economic downturn, which could result in a larger customer turnover than is currently anticipated, reduced demand for our products and services, and increased length of

sales cycles, in which case our revenues could be significantly impacted. The impact of the COVID-19 pandemic may also exacerbate other risks discussed in this "Risk Factors" section and elsewhere in this prospectus. It is not possible at this time to estimate the impact that the COVID-19 pandemic could have on our business, as the impact will depend on future developments, which are highly uncertain and cannot be predicted.

If organizations do not adopt cloud-enabled, and/or SaaS-delivered cybersecurity solutions that may be based on new and untested security concepts, our ability to grow its business and results of operations may be adversely affected.

Our future success depends on the growth in the market for cloud-enabled and/or SaaS-delivered cybersecurity solutions. The use of SaaS solutions to manage and automate security and IT operations is rapidly evolving. As such, it is difficult to predict its potential growth, customer adoption and retention rates, customer demand for our solutions, or the success of existing or future competitive products. Any expansion in our market depends on a number of factors, including the cost, performance and perceived value associated with its solutions and those of its competitors. If our solutions do not achieve widespread adoption or there is a reduction in demand for our solutions due to a lack of customer acceptance, technological challenges, competing products, privacy or other liability concerns, decreases in corporate spending, weakening economic conditions, or otherwise, it could adversely affect our business, results of operations and financial results, resulting from such things as early terminations, reduced customer retention rates, or decreased sales. We do not know whether the trend in adoption of cloud- enabled and/or SaaS-delivered cybersecurity solutions that we have experienced in the past will continue in the future. Furthermore, if we or other SaaS security providers experience security incidents, loss, or disclosure of customer data, disruptions in delivery, or other problems, the market for SaaS solutions as a whole, including our security solutions, could be negatively affected.

In addition to reliance on a cloud-enabled and/or SaaS-delivered model, our cybersecurity utilize a novel and relatively new approach to collective defense that relies on customers sharing sensitive customer information with us. Some of that raw customer information may contain personal or confidential information, or data perceived to be personal or confidential information. From that customer information, we generate analytics that allow us to deliver threat knowledge and network intelligence at machine speed across a wide variety of industries. Because this new approach requires the sharing of sensitive customer information, concerns may exist that sharing of the customer information may violate, or be perceived as potentially violating, privacy laws or providing a competitive advantage to another entity. As a result, some current or prospective customers may decide not to procure our products or share any customer information. Such lack of acceptance could have negative effects on us, including reduced or lost revenues or inadequate information being available for our analysis, thus making our products less effective. In addition, uncertainties about the regulatory environment concerning personal information and the potential liability raised by sharing such information could further inhibit the broad-scale adoption of our solutions.

Historically, information sharing related to cybersecurity has been a very well accepted concept from a theoretical perspective but very difficult to implement in practice. Companies are generally reluctant to share their sensitive cyber information with other entities, despite knowing the advantages of doing so. Although raw customer information will not be shared with other parties, it does undergo filtering, concatenation, and other transformations within our solutions with the goal of removing any sensitive or personal information. Misperceptions may exist, however, about what information gets shared, with whom that information is shared, and the jurisdictions (including foreign countries) of the companies with which the information gets shared. Further, concerns of existing or potential customers may exist related to the ability to completely remove any indicia of the source company, general market rejection of information sharing, or specific market skepticism of our approach to collective defense, which may further add to a lack of customer acceptance.

In addition to the potential concerns related to sharing sensitive information in a system consisting of commercial or potentially competitive entities, additional concerns can arise when governments become involved as participants in the collective defense ecosystem. From a commercial perspective, companies frequently view

information sharing with governments as risky, based on perceptions that the governments might use such shared information to take action against the companies or to otherwise utilize it in a way that will expose such companies to liability. Such perceptions could lead commercial entities to stop sharing, not procure our services in the first place, or terminate their relationship with us altogether. Similarly, governments (as customers) may be unable to properly process such data or utilize it in a meaningful way, or share useful information back into our solutions. Any of these concerns could lead to reduced sales or contribute to a lack of customer acceptance. In addition, the mere involvement of one or more government entities may harm our reputation with certain companies.

If we are unable to attract new customers, our future results of operations could be harmed.

To expand our customer base, we will need to convince potential customers to allocate a portion of their discretionary budgets to purchase our platform and solutions. Our sales efforts have often involved educating our prospective customers about the uses and benefits of our platform and solutions. Enterprises and governments that use legacy security products, such as signature-based or malware-focused products, firewalls, intrusion prevention systems and endpoint technologies, may be hesitant to purchase our platform and solutions if they believe that legacy security products are more cost effective, provide substantially the same functionality as our platform and solutions or provide a level of cybersecurity that is sufficient to meet their needs.

We may have difficulty convincing prospective customers of the value of adopting our solutions. Even if we are successful in convincing prospective customers that a cloud-enabled platform like ours is critical to protect against cyberattacks, they may not decide to purchase our platform and solutions for a variety of reasons, some of which are out of our control. For example, any future deterioration in general economic conditions, including a downturn due to the outbreak of diseases such as COVID-19, may cause our current and prospective customers to cut their overall security and IT operations spending, and such cuts may fall disproportionately on cloud-based security solutions. Economic weakness, customer financial difficulties, and constrained spending on security and IT operations may result in decreased revenue and adversely affect our results of operations and financial condition. Additionally, if the incidence of cyberattacks were to decline, or enterprises or governments perceive that the general level or relative risk of cyberattacks has declined, our ability to attract new customers and expand sales of our solutions to existing customers could be adversely affected. If organizations do not continue to adopt our platform and solutions, our sales will not grow as quickly as anticipated, or at all, and our business, results of operations, and financial condition would be harmed.

If our customers do not renew their subscriptions for our products, our future results of operations could be harmed.

In order for us to maintain or improve our results of operations, it is important that our customers renew their subscriptions for our platform and solutions when existing contract terms expire, and that we expands our commercial relationships with our existing customers by selling additional subscriptions. Our customers have no obligation to renew their subscriptions after the expiration of their contractual subscription period, which is generally one year, and in the normal course of business, some customers have elected not to renew. In addition, our customers may renew for shorter contract subscription lengths or cease using certain solutions. Our customer retention and expansion may decline or fluctuate as a result of a number of factors, including its customers' satisfaction with our services, our pricing, customer security and networking issues and requirements, our customers' spending levels, mergers and acquisitions involving our customers, industry developments, competition and general economic conditions. If our efforts to maintain and expand our relationships with our existing customers are not successful, our business, results of operations, and financial condition may materially suffer.

- errors, defects, or performance problems in our software, including third-party or open-source software incorporated in our software;
- improper deployment or configuration of our solutions;
- the failure of its redundancy systems, in the event of a service disruption at one of our data centers, to provide failover to other data centers in our data center network;
- the failure of our disaster recovery and business continuity arrangements; and
- effects of third-party software updates with hidden malware, similar to the supply chain attack that occurred via SolarWinds.

The adverse effects of any service interruptions on our reputation, results of operations, and financial condition may be disproportionately heightened due to the nature of our business and the fact that our customers have a low tolerance for interruptions of any duration. Interruptions or failures in our service delivery could result in a cyberattack or other security threat to one of our customers during such periods of interruption or failure. Additionally, interruptions or failures in our service could cause customers to terminate their subscriptions, adversely affect renewal rates, and harm our ability to attract new customers. Our business would also be harmed if our customers believe that a cloud-enabled and/or SaaS- delivered cybersecurity solution is unreliable. We may experience service interruptions and other performance problems due to a variety of factors. The occurrence of any of these factors, or if it is unable to rapidly and cost-effectively fix such errors or other problems that may be identified, could damage its reputation, negatively affect our relationship with our customers or otherwise harm our business, results of operations and financial condition.

If we do not effectively expand and train our direct sales force, we may be unable to add new customers or increase sales to existing customers, and our business will be adversely affected.

We depend on our direct sales force to obtain new customers and increase sales with existing customers. Our ability to achieve significant revenue growth will depend, in large part, on our success in recruiting, training and retaining sufficient numbers of sales personnel, particularly in international markets. We have expanded our sales organization significantly in recent periods and expect to continue to add additional sales capabilities in the near term. There is significant competition for sales personnel with the skills and technical knowledge that we require. New hires require significant training and may take significant time before they achieve full productivity, and this delay is accentuated by our long sales cycles. Our recent hires and planned hires may not become productive as quickly as we expect, and we may be unable to hire or retain sufficient numbers of qualified individuals in the markets where we do business or plans to do business. In addition, a large percentage of our salesforce is new to our business and selling our solutions, and therefore this team may be less effective than our more seasoned sales personnel. Furthermore, hiring sales personnel in new countries, or expanding our existing presence, requires upfront and ongoing expenditures that we may not recover if the sales personnel fail to achieve full productivity. We cannot predict whether, or to what extent, our sales will increase as we expand our sales force or how long it will take for sales personnel to become productive. If we are unable to hire and train a sufficient number of effective sales personnel, or the sales personnel we hire are not successful in obtaining new customers or increasing sales to our existing customer base, our business and results of operations will be adversely affected.

Because we recognize revenue from subscriptions to our platform and other forms of providing customers with access to our software over the term of the subscription or contract, downturns or upturns in new business will not be immediately reflected in our results of operations.

We generally recognize revenue from customers ratably over the terms of their subscription or contract term, which average over three years in length, though may be as short as one year or less. As a result, a substantial portion of the revenue that we report in each period is attributable to the recognition of deferred revenue relating to agreements that we entered into during previous periods. Consequently, any increase or decline in new sales or renewals in any one period will not be immediately reflected in our revenue for that period. Any such change,

however, would affect our revenue in future periods. Accordingly, the effect of downturns or upturns in new sales and potential changes in our rate of renewals may not be fully reflected in our results of operations until future periods.

A limited number of customers represent a substantial portion of our revenue. If we fail to retain these customers, our revenue could decline significantly.

We derive a substantial portion of our revenue from a limited number of customers. For the years ended January 31, 2021 and 2020, six customers accounted for 46% or $13,381 with one of those customers accounting for 10% and four customers accounted for 48% or $11,187 with all four being over 10% of the Company's revenue, respectively. As of July 31, 2021 and January 31, 2021, two and three customers represented 68% and 85%, respectively, of our total accounts receivable balance. Significant customers are those which represent at least 10% of our total revenue at each respective period ending date. The following table presents customers that represented 10% or more of our total annual revenue:

	Year Ended January 31,	
	2021	2020
Customer A	10%	*
Customer B	*	14%
Customer C	*	10%
Customer D	*	10%
Customer E	*	14%

* Less than 10%

For the six months ended July 31, 2021, two significant customers accounted for 22% of our revenues. The following table presents customers that represented 10% or more of our total revenue for the six months ended July 31, 2021 and 2020:

	Six Months Ended July 31,	
	2021	2020
Customer A	*	10%
Customer E	11%	*
Customer F	*	10%
Customer G	11%	*
	22%	20%

* Less than 10%

As a result, our revenue could fluctuate materially and could be materially and disproportionately impacted by purchasing decisions of these customers or any other significant future customer. Any of our significant customers may decide to purchase less than they have in the past, may alter their purchasing patterns at any time with limited notice, or may decide not to continue to license our products at all, any of which could cause our revenue to decline and adversely affect our financial condition and results of operations. If we do not further diversify our customer base, we will continue to be susceptible to risks associated with customer concentration.

Our results of operations may fluctuate significantly, which could make our future results difficult to predict and could cause our results of operations to fall below expectations.

Our results of operations have varied significantly from period to period, and we expect that our results of operations will continue to vary as a result of a number of factors, many of which are outside of our control and may be difficult to predict, including:

- the impact of the COVID-19 pandemic on our operations, financial results, and liquidity and capital resources, including on customers, sales, expenses, and employees;

- our ability to attract new and retain existing customers;
- the budgeting cycles, seasonal buying patterns, and purchasing practices of customers;
- the timing and length of our sales cycles;
- changes in customer or distribution partner requirements or market needs;
- changes in the growth rate of our market;
- the timing and success of new product and service introductions by us or our competitors or any other competitive developments, including consolidation among our customers or competitors;
- the level of awareness of cybersecurity threats, particularly advanced cyberattacks, and the market adoption of our platform;
- our ability to successfully expand our business domestically and internationally;
- decisions by organizations to purchase security solutions from larger, more established security vendors or from their primary IT equipment vendors;
- changes in our pricing policies or those of our competitors;
- any disruption in our relationship with distribution partners;
- insolvency or credit difficulties confronting our customers, affecting their ability to purchase or pay for our solutions;
- significant security breaches of, technical difficulties with or interruptions to, the use of our platform;
- extraordinary expenses such as litigation or other dispute-related settlement payments or outcomes;
- general economic conditions, both in domestic and foreign markets;
- future accounting pronouncements or changes in our accounting policies or practices;
- negative media coverage or publicity;
- political events;
- the amount and timing of operating costs and capital expenditures related to the expansion of our business; and
- increases or decreases in expenses caused by fluctuations in foreign currency exchange rates.

In addition, we experience seasonal fluctuations in our financial results as we can receive a higher percentage of our annual orders from new customers, as well as renewal orders from existing customers, in the fourth fiscal quarter as compared to other quarters due to the annual budget approval process of many of our customers. Any of the above factors, individually or in the aggregate, may result in significant fluctuations in our financial and other results from period to period. As a result of this variability, our historical results of operations should not be relied upon as an indication of future performance. Moreover, this variability and unpredictability could result in our failure to meet our operating plan or the expectations of investors or analysts for any period. If we fail to meet such expectations for these or other reasons, our stock price could fall substantially, and we could face costly lawsuits, including securities class action suits.

Our sales cycles can be long and unpredictable, and our sales efforts require considerable time and expense.

Our revenue recognition is difficult to predict because of the length and unpredictability of the sales cycle for our platform, particularly with respect to large organizations and government entities. Customers often view the subscription to our platform as a significant strategic decision and, as a result, frequently require considerable time to evaluate, test, and qualify our platform and solutions prior to entering into or expanding a relationship with us. Large enterprises and government entities in particular often undertake a significant evaluation process that further lengthens our sales cycle.

Our direct sales team develops relationships with our customers, and works with our distribution partners on account penetration, account coordination, sales and overall market development. We spend substantial time and resources on our sales efforts without any assurance that our efforts will produce a sale. Security solution purchases are frequently subject to budget constraints, multiple approvals, and unanticipated administrative, processing, and other delays. As a result, it is difficult to predict whether and when a sale will be completed. The failure of our efforts to secure sales after investing resources in a lengthy sales process could adversely affect our business and results of operations.

We rely heavily on the services of our senior management team, and if we are not successful in attracting or retaining senior management personnel, we may not be able to successfully implement our business strategy.

Our future success will be substantially dependent on our ability to attract, retain, and motivate the members of its management team. In particular, we will be highly dependent on the services of Gen. Keith B. Alexander (Ret.) and William Welch, our co-chief executive officers, who will be critical to our future vision and strategic direction. We will also rely on our leadership team in the areas of operations, security, analytics, engineering, product management, research and development, marketing, sales, partnerships, mergers and acquisitions, support, and general and administrative functions. Gen. Alexander is important to our future growth as he provides access to key decisionmakers within government agencies and the private sector, and his leadership role would be difficult to replace. Although we expect that we will enter into new employment agreements with some of our key personnel, our employees, including our executive officers, will be employed on an "at-will" basis, which means they may terminate their employment with us at any time. If one or more of our key employees resigns or otherwise ceases to provide us with their service, our business could be harmed.

If we are unable to attract and retain qualified personnel, our business could be harmed.

There is significant competition for personnel with the skills and technical knowledge that we will require across our technology, cyber, sales, professional services and administrative support functions. Competition for these personnel in the Washington, D.C. metro area, where our corporate headquarters is located, and in other locations where we maintain offices or otherwise operate, is competitive, especially for experienced sales professionals, engineers and data scientists experienced in designing and developing cybersecurity software. Although our current remote work environment facilitates our ability to attract talent across a wider geographic base, we have from time to time experienced, and we expect to continue to experience, difficulty in hiring and retaining employees with appropriate qualifications. Many of the companies with which we compete for experienced personnel have greater resources than us. Our competitors also may be successful in recruiting and hiring members of our management team or other key employees, and it may be difficult for us to find suitable replacements on a timely basis, on competitive terms, or at all. We may also be subject to allegations that employees we hire have been improperly solicited, or that they have divulged proprietary or other confidential information or that their former employers own such employees' inventions or other work product, or that they have been hired in violation of non-compete provisions or non-solicitation provisions.

In addition, job candidates and existing employees often consider the value of the equity awards they receive in connection with their employment. Volatility or lack of performance in our stock price may also affect our ability to attract and retain key employees. Some of our employees will become vested in a substantial amount of equity awards, which may give them a material amount of personal wealth. This may make it more difficult for us to retain and motivate these employees, and this wealth could affect their decision about whether or not they continue to work for us. Any failure to successfully attract, integrate or retain qualified personnel to fulfill our current or future needs could adversely affect our business, results of operations and financial condition.

If we are not able to maintain and enhance our brand and our reputation as a provider of high-efficacy cybersecurity solutions, our business and results of operations may be adversely affected.

We believe that maintaining and enhancing our brand and our reputation as a provider of high-efficacy cybersecurity solutions is critical to our relationship with our existing customers and distribution partners and our

ability to attract new customers and partners. The successful promotion of our brand will depend on a number of factors, including our investment in marketing efforts, our ability to continue to develop additional features for our platform, our ability to successfully differentiate our platform from competitive cloud-enabled or legacy security solutions and, ultimately, our ability to detect and remediate cyberattacks. Although we believe it is important for our growth, these brand promotion activities may not be successful or yield increased revenue.

In addition, independent industry or financial analysts and research firms often test our solutions and provide reviews of our platform, along with the products of our competitors, and perception of our platform in the marketplace may be significantly influenced by these reviews. If these reviews are negative, or less positive as compared to those of our competitors' products, our brand may be adversely affected. Our solutions may fail to detect or prevent threats in any particular test for a number of reasons that may or may not be related to the efficacy of our solutions in real world environments. To the extent potential customers, industry analysts, or testing firms believe that the occurrence of a failure to detect or prevent any particular threat is a flaw or indicates that our solutions or services do not provide significant value, we may lose customers, and our reputation, financial condition, and business would be harmed. Additionally, the performance of our distribution partners may affect its brand and reputation if customers do not have a positive experience with these partners. In addition, we have in the past worked, and we will continue to work, with high profile customers as well as assist in analyzing and remediating high profile cyberattacks. This work with such customers and cyberattacks may expose us to negative publicity and media coverage. Negative publicity, including about the efficacy and reliability of our platform, its products offerings, our professional services and the customers we work with, even if inaccurate, could adversely affect our reputation and brand.

If we are unable to maintain successful relationships with our distribution partners, or if our distribution partners fail to perform, our ability to market, sell and distribute our platform and solutions efficiently will be limited, and our business, financial position and results of operations will be harmed.

In addition to its direct sales force, we rely on certain key distribution partners to sell and support our platform. An increasing amount of our sales flow through our distribution partners, and we expect our reliance on such partners to continue to grow for the foreseeable future. Additionally, we have entered into, and we intend to continue to enter into, partnerships with third parties to support our future growth plans. The loss of a substantial number of distribution partners, or the failure to recruit additional partners, could adversely affect our results of operations. Our ability to achieve revenue growth in the future will depend in part on its success in maintaining successful relationships with our distribution partners and in training them to independently sell and deploy our platform. If we fail to effectively manage our existing sales channels, or if our distribution partners are unsuccessful in fulfilling the orders for our solutions, or if we are unable to recruit and retain a sufficient number of high quality distribution partners who are motivated to sell our products, our ability to sell our products and results of operations will be harmed.

Our business depends, in part, on sales to government organizations, and significant changes in the contracting or fiscal policies of such government organizations could have an adverse effect on our business and results of operations.

Our future growth depends, in part, on increasing sales to government organizations. Demand from government organizations is often unpredictable, subject to budgetary uncertainty and typically involves long sales cycles. We have made significant investments to address the government sector, but we cannot assure you that these investments will be successful, or that we will be able to maintain or grow our revenue from the government sector. Although we anticipate that they may increase in the future, sales to U.S. federal, state and local governmental agencies have not accounted for, and may never account for, a significant portion of our revenue. U.S. federal, state and local government sales are subject to a number of challenges and risks that may adversely impact our business. Sales to such government entities include the following risks:

- selling to governmental agencies can be highly competitive, expensive and time-consuming, often requiring significant upfront time and expense without any assurance that such efforts will generate a sale;

- government certification requirements applicable to our products may change and, in doing so, restrict our ability to sell into the U.S. federal government sector until it has attained the required certifications.
- government demand and payment for our platform may be impacted by public sector budgetary cycles and funding authorizations, with funding reductions or delays adversely affecting public sector demand for our platform;
- governments routinely investigate and audit government contractors' administrative processes, and any unfavorable audit could result in the government refusing to continue buying our platform, which would adversely impact our revenue and results of operations, or institute fines or civil or criminal liability if the audit were to uncover improper or illegal activities;
- interactions with the U.S. federal government may be limited by post-employment ethics restrictions on members of our management;
- foreign governments may have concerns with purchasing security products from a company that employs former NSA employees and officials, which may negatively impact sales; and
- governments may require certain products to be manufactured, hosted, or accessed solely in their country or in other relatively high-cost manufacturing locations, and we may not manufacture all products in locations that meet these requirements, affecting its ability to sell these products to governmental agencies.

We have achieved Federal Risk and Authorization Management Program ("**FedRAMP**") "FedRAMP- ready" status, but such status is only available for a certain period of time before which it must be utilized. If not utilized, we would likely have to go through certain parts of the FedRAMP process again in order to sell its products to government agencies. Moreover, even if we were to achieve FedRAMP-certified status, such certification is costly to maintain, and if we were to lose such a certification in the future it would restrict its ability to sell to government customers. It is also possible that additional guidelines and/or certifications, such as the Cybersecurity Maturity Model Certification ("**CMMC**"), will be required to expand participation in the government sectors.

The occurrence of any of the foregoing could cause governments and governmental agencies to delay or refrain from purchasing our solutions in the future or otherwise have an adverse effect on our business and results of operations.

We may not scale and adapt our existing technology in a timely and cost-effective manner to meet our customers' performance and other requirements.

Our future growth will be dependent upon our ability to continue to meet the needs of new customers and the expanding needs of our existing customers as their use of our solutions grows. As our customers gain more experience with our solutions, the number of events, the amount of data transferred, processed, and stored by it, the number of locations where its platform and services are being accessed, have in the past, and may in the future, expand rapidly. In order to meet the performance and other requirements of our customers, we intend to continue to make significant investments to increase capacity and to develop and implement new technologies in our service and cloud infrastructure operations. These technologies, which include databases, applications, and server optimizations, network and hosting strategies, and automation, are often advanced, complex, new, and untested. We may not be successful in developing or implementing these technologies. In addition, it takes a significant amount of time to plan, develop, and test improvements to our technologies and infrastructure, and we may not be able to accurately forecast demand or predict the results it will realize from such improvements. To the extent that we do not effectively scale our operations to meet the needs of our growing customer base and to maintain performance as our customers expand their use of our solutions, we may not be able to grow as quickly as anticipated, customers may reduce or cancel use of our solutions and we may be unable to compete as effectively and its business and results of operations may be harmed.

claims could result in litigation. Litigation could be costly to defend, have a negative effect on our results of operations and financial condition or require us to devote additional research and development resources to change our solutions. Responding to any infringement or noncompliance claim by an open source vendor, regardless of our validity, discovering certain open source software code in our platform, or a finding that we have breached the terms of an open source software license, could harm our business, results of operations and financial condition, by, among other things:

- resulting in time-consuming and costly litigation;
- diverting management's time and attention from developing our business;
- requiring us to pay monetary damages or enter into royalty and licensing agreements that we would not normally find acceptable;
- causing delays in the deployment of its platform or service offerings to our customers;
- requiring us to stop offering certain services or features of our platform;
- requiring us to redesign certain components of our platform using alternative non-infringing or non-open source technology, which could require significant effort and expense;
- requiring us to disclose its software source code and the detailed program commands for our software;
- prohibiting us from charging license fees for the proprietary software that uses certain open source; and
- requiring us to satisfy indemnification obligations to our customers.

We provide service level commitments under some of our customer contracts. If we fail to meet these contractual commitments, we could be obligated to provide credits for future service and our business could suffer.

Certain of our customer agreements contain service level commitments, which contain specifications regarding the availability and performance of our platform. Any failure of or disruption to our infrastructure could impact the performance of our platform and the availability of services to customers. If we are unable to meet our stated service level commitments or if we suffer extended periods of poor performance or unavailability of our platform, we may be contractually obligated to provide affected customers with service credits for future subscriptions, and, in certain cases, refunds. To date, there has not been a material failure to meet our service level commitments, and we do not currently have any material liabilities accrued on our balance sheet for such commitments. However, our revenue, other results of operations and financial condition could be harmed if we suffer performance issues or downtime that exceeds the service level commitments under our agreements with our customers.

We may become involved in litigation that may adversely affect us.

We may be subject to claims, suits and government investigations and other proceedings including patent, product liability, class action, whistleblower, personal injury, property damage, labor and employment, commercial disputes, compliance with laws and regulatory requirements and other matters, and we may become subject to additional types of claims, suits, investigations and proceedings as our business develops. While we believe that we have acted in compliance in all material respects with applicable antitrust laws, such investigation, as well as any other claims, suits, and government investigations and proceedings that may be asserted against us in the future, are inherently uncertain and their results cannot be predicted with certainty. Regardless of the outcome, any of these types of legal proceedings can have an adverse impact on us because of legal costs and diversion of management attention and resources, and could cause us to incur significant expenses or liability, adversely affect our brand recognition, and/or require us to change its business practices. The expense of litigation and the timing of this expense from period to period are difficult to estimate, subject to change and could adversely affect our results of operations. It is possible that a resolution of one or more such

proceedings could result in substantial damages, settlement costs, fines and penalties that could adversely affect its business, consolidated financial position, results of operations, or cash flows in a particular period. These proceedings could also result in reputational harm, sanctions, consent decrees, or orders requiring a change in our business practices. Because of the potential risks, expenses and uncertainties of litigation, we may, from time to time, settle disputes, even where we have meritorious claims or defenses, by agreeing to settlement agreements. Because litigation is inherently unpredictable, we cannot assure you that the results of any of these actions will not have a material adverse effect on our business, financial condition, results of operations, and prospects.

Our ability to maintain customer satisfaction will depend in part on the quality of our customer support.

Once our platform is deployed within our customers' networks, our customers depend on our customer support services to resolve any issues relating to implementation and maintenance of the platform. If we do not provide effective ongoing support, our ability to sell additional subscriptions to existing customers would be adversely affected and our reputation with potential customers could be damaged. Many larger organizations have more complex networks and require higher levels of support than smaller customers. Failure to maintain high-quality customer support could also have a material adverse effect on our business, results of operations and financial condition.

We may need to raise additional capital to maintain and expand our operations and invest in new solutions, which capital may not be available on terms acceptable to us, or at all, and which could reduce our ability to compete and could harm our business.

Retaining or expanding our current levels of personnel and products offerings may require additional funds to respond to business challenges, including the need to develop new products and enhancements to our platform, improve our operating infrastructure, or acquire complementary businesses and technologies. The failure to raise additional capital or generate the significant capital necessary to expand our operations and invest in new products could reduce our ability to compete and could harm our business. Accordingly, we may need to engage in additional equity or debt financings to secure additional funds. If we raise additional equity financing, stockholders may experience significant dilution of their ownership interests and the market price of the common stock could decline. If we engage in debt financing, the holders of debt would have priority over the holders of common stock, and we may be required to accept terms that restrict our operations or our ability to incur additional indebtedness or to take other actions that would otherwise be in the interests of the debt holders. Any of the above could harm our business, results of operations and financial condition.

Our business is subject to the risks of warranty claims, product returns, product liability, and product defects from real or perceived defects in our solutions or their misuse by customers or third parties, and indemnity provisions in various agreements potentially expose we to substantial liability for intellectual property infringement and other losses.

We may be subject to liability claims for damages related to errors or defects in our solutions. A material liability claim or other occurrence that harms our reputation or decreases market acceptance of its products may harm its business and results of operations. Although we generally has limitations of liability provisions in its terms and conditions of sale, these provisions may not fully or effectively protect us from claims as a result of federal, state, or local laws or ordinances, or unfavorable judicial decisions in the United States or other countries. These provisions may also be negotiated to varying levels with different customers. The sale and support of products also entails the risk of product liability claims.

Additionally, our agreements with customers and other third parties typically include indemnification or other provisions under which we agree to indemnify or otherwise be liable to them for losses suffered or incurred as a result of claims regarding intellectual property infringement, breach of agreement, including confidentiality, privacy and security obligations, violation of applicable laws, damages caused by failures of our solutions or to property or persons, or other liabilities relating to or arising from our products and services, or other acts or

omissions. These contractual provisions often survive termination or expiration of the applicable agreement. We have not to date received any indemnification claims from third parties. However, as we continue to grow, the possibility of these claims against us will increase. Large indemnity obligations, whether for intellectual property or other claims, could harm our business, results of operations and financial condition.

Additionally, our platform and solutions may be used by our customers and other third parties who obtain access to its solutions for purposes other than for which the platform was intended. For example, the platform might be misused by a customer to monitor our employee's activities in a manner that violates the employee's privacy rights under applicable law.

During the course of performing certain solution-related services and professional services, our teams may have significant access to its customers' networks. We cannot be sure that a disgruntled employee may not take advantage of such access, which may make its customers vulnerable to malicious activity by such employee. Any such misuse of our platform could result in negative press coverage and negatively affect its reputation, which could result in harm to our business, reputation and results of operations.

We maintain insurance to protect against certain claims associated with the use of our products, but our insurance coverage may not adequately cover any claim asserted against us. In addition, even claims that ultimately are unsuccessful could result in the expenditure of funds in litigation, divert management's time and other resources, and harm our business and reputation.

Future acquisitions, strategic investments, partnerships, or alliances could be difficult to identify and integrate, divert the attention of key management personnel, disrupt our business, dilute stockholder value and adversely affect our results of operations and financial condition.

As part of its business strategy, we have in the past made, and we are likely to continue to make, investments in and/or acquire complementary companies, services, or technologies. The ability to acquire and integrate other companies, services or technologies in a successful manner in the future is not guaranteed. We may not be able to find suitable acquisition candidates, and we may not be able to complete such acquisitions on favorable terms, if at all. If we do complete acquisitions, we may not ultimately strengthen our competitive position or ability to achieve our business objectives, and any acquisitions we complete could be viewed negatively by our customers or investors. In addition, if we are unsuccessful at integrating such acquisitions, or the technologies associated with such acquisitions, our revenue and results of operations could be adversely affected. Any integration process may require significant time and resources, and we may not be able to manage the process successfully. We may not successfully evaluate or utilize the acquired technology or personnel, or accurately forecast the financial impact of an acquisition transaction, including accounting charges. We may have to pay cash, incur debt or issue equity securities to pay for any such acquisition, each of which could adversely affect its financial condition and the market price of our common stock. The sale of equity or issuance of debt to finance any such acquisitions could result in dilution to stockholders. The incurrence of indebtedness would result in increased fixed obligations and could also include covenants or other restrictions that would impede our ability to manage our operations.

Additional risks we may face in connection with acquisitions include:

- diversion of management time and focus from operating our business to addressing acquisition integration challenges;
- coordination of engineering, analytics, research and development, operations, and sales and marketing functions;
- integration of product and service offerings;
- retention of key employees from the acquired company;

- changes in relationships with strategic partners as a result of product acquisitions or strategic positioning resulting from the acquisition;
- cultural challenges associated with integrating employees from the acquired company into the organization;
- integration of the acquired company's accounting, management information, human resources and other administrative systems;
- the need to implement or improve controls, procedures, and policies at a business that prior to the acquisition may have lacked sufficiently effective controls, procedures and policies;
- financial reporting, revenue recognition or other financial or control deficiencies of the acquired company that are not adequately addressed and that cause our reported results to be incorrect;
- liability for activities of the acquired company before the acquisition, including intellectual property infringement claims, violations of laws, commercial disputes, tax liabilities and other known and unknown liabilities;
- unanticipated write-offs or charges; and
- litigation or other claims in connection with the acquired company, including claims from terminated employees, customers, former stockholders or other third parties.

The failure to address these risks or other problems encountered in connection with acquisitions and investments could cause us to fail to realize the anticipated benefits of these acquisitions or investments, cause us to incur unanticipated liabilities, and harm our business generally.

If we cannot maintain our company culture as we grow, we could lose the innovation, teamwork, passion and focus on execution that have contributed to our success, and our business may be harmed.

We believe that our corporate culture has been a contributor to our success, which we believe fosters innovation, teamwork, passion and focus on building and marketing its platform. As we grow and develops the infrastructure of a public operating company, it may be difficult to maintain our corporate culture. Any failure to preserve that culture could harm our future success, including our ability to retain and recruit personnel, innovate and operate effectively and execute on our business strategy. Additionally, our productivity and the quality of our solutions may be adversely affected if we do not integrate and train new employees quickly and effectively. If we experience any of these effects in connection with future growth, it could impair our ability to attract new customers, retain existing customers and expand their use of our platform, all of which would adversely affect our business, financial condition and results of operations.

Our international operations and plans for future international expansion expose us to significant risks, and failure to manage those risks could adversely impact our business.

We derived 39% and 14% of its total revenue from its international customers for fiscal 2021 and fiscal 2020, respectively. our growth strategy includes expansion into target geographies, but there is no guarantee that such efforts will be successful. We expect that our international activities will continue to grow in the future, as we continue to pursue opportunities in international markets. These international operations will require significant management attention and financial resources and are subject to substantial risks, including:

- greater difficulty in negotiating contracts with standard terms, enforcing contracts, and managing collections, including longer collection periods;
- higher costs of doing business internationally, including costs incurred in establishing and maintaining office space and equipment for international operations and creating international operating entities, where applicable;

- management communication and integration problems resulting from cultural and geographic dispersion;
- risks associated with trade restrictions and foreign legal requirements, including any importation, certification, and localization of our platform that may be required in foreign countries;
- greater risk of unexpected changes in applicable foreign laws, regulatory practices, tariffs, and tax laws and treaties;
- compliance with anti-bribery laws, including the U.S. Foreign Corrupt Practices Act of 1977, as amended, the U.S. Travel Act and the UK Bribery Act 2010, violations of which could lead to significant fines, penalties, and collateral consequences;
- heightened risk of unfair or corrupt business practices in certain geographies and of improper or fraudulent sales arrangements that may impact financial results and result in restatements of, or irregularities in, financial statements;
- the uncertainty of protection for intellectual property rights in some countries;
- general economic and political conditions in these foreign markets;
- foreign exchange controls or tax regulations that might prevent us from repatriating cash earned outside the United States;
- political and economic instability in some countries;
- the potential for foreign government demands for access to information or corporate property;
- double taxation of international earnings and potentially adverse tax consequences due to changes in the tax laws of the United States or the foreign jurisdictions in which we operate;
- unexpected costs for the localization of services, including translation into foreign languages and adaptation for local practices and regulatory requirements;
- requirements to comply with foreign privacy, data protection, and information security laws and regulations and the risks and costs of noncompliance;
- greater difficulty in identifying, attracting and retaining local qualified personnel, and the costs and expenses associated with such activities;
- greater difficulty identifying qualified distribution partners and maintaining successful relationships with such partners;
- differing employment practices and labor relations issues; and
- difficulties in managing and staffing international offices and increased travel, infrastructure, and legal compliance costs associated with multiple international locations.

Additionally, all of our sales contracts are currently denominated in U.S. dollars. However, a strengthening of the U.S. dollar could increase the cost of our solutions to our international customers, which could adversely affect our business and results of operations. In addition, an increasing portion of operating expenses is expected to be incurred outside the United States and denominated in foreign currencies, and will be subject to fluctuations due to changes in foreign currency exchange rates. If we become more exposed to currency fluctuations and are not able to successfully hedge against the risks associated with currency fluctuations, our results of operations could be adversely affected.

As we continue to develop and grow our business globally, our success will depend in large part on our ability to anticipate and effectively manage these risks. The expansion of our existing international operations and entry into additional international markets will require significant management attention and financial resources. Our failure to successfully manage international operations and the associated risks could limit the future growth of our business.

Our ability to use our net operating loss carryforwards and certain other tax attributes may be limited.

As of January 31, 2021, we had aggregate U.S. federal and state net operating loss carryforwards of $154.9 million and $100.0 million, respectively, which may be available to offset future taxable income for income tax purposes.

U.S. federal net operating loss carryforwards generated in taxable years beginning before January 1, 2018 may be carried forward for 20 years to offset future taxable income. Under tax legislation commonly referred to as the Tax Cuts and Jobs Act (the "**Tax Act**"), as modified by the Coronavirus Aid, Relief, and Economic Security Act (the "**CARES Act**"), U.S. federal net operating losses generated in taxable years beginning after December 31, 2017, can be carried forward indefinitely, but the deductibility of such net operating loss carryforwards in taxable years beginning after December 31, 2020 is limited to 80% of taxable income. It is uncertain if and to what extent various states will conform their tax laws and regulations to the Tax Act or the CARES Act.

If not utilized, $25.3 million of our U.S. federal net operating loss carryforwards expire on various dates through 2037 and $129.7 million are able to be carried forward indefinitely under current law. Realization of these net operating loss carryforwards depends on future taxable income, and there is a risk that, even if we achieve profitability, our existing carryforwards could expire unused or be subject to limitations and be unavailable to offset future income tax liabilities, which could adversely affect our results of operations.

In addition, under Sections 382 and 383 of the Internal Revenue Code of 1986, as amended (the "**Code**"), if a corporation undergoes an "ownership change," generally defined as a greater than 50% change (by value) in ownership by "5 percent shareholders" over a rolling three-year period, the corporation's ability to use its pre-change net operating loss carryovers and other pre-change tax attributes to offset its post-change income or taxes may be limited. We may experience ownership changes in the future as a result of shifts in its stock ownership (which may be outside of its control). In addition, at the state level, there may be periods during which the use of net operating loss carryforwards is suspended or otherwise limited, which could accelerate or permanently increase state taxes owed. As a result, if we earn net taxable income, our ability to use pre-change net operating loss carryforwards to offset U.S. federal taxable income may be subject to limitations, which could potentially result in increased future tax liability to us.

Taxing authorities may successfully assert that we should have collected or in the future should collect sales and use, value added or similar taxes, and we could be subject to liability with respect to past or future sales, which could adversely affect our results of operations.

We do not collect sales and use, value added or similar taxes in all jurisdictions in which we have sales because we have been advised that such taxes are not applicable to our services in certain jurisdictions. Sales and use, value added, and similar tax laws and rates vary greatly by jurisdiction. Certain jurisdictions in which we do not collect such taxes may assert that such taxes are applicable, which could result in tax assessments, penalties and interest, to us or our customers for the past amounts, and we may be required to collect such taxes in the future. If we are unsuccessful in collecting such taxes from our customers, we could be held liable for such costs, which may adversely affect our results of operations.

Our operations and intercompany arrangements will be subject to the tax laws of various jurisdictions, and we could be obligated to pay additional taxes, which would harm our results of operations.

We will expand our international operations and staff to support our business in international markets. We expect that we will generally conduct international operations through wholly owned subsidiaries and may be required to report our taxable income in various jurisdictions worldwide based upon its business operations in those jurisdictions. Our intercompany relationships will be subject to complex transfer pricing regulations administered by taxing authorities in various jurisdictions. The amount of taxes paid in different jurisdictions may depend on the application of the tax laws of the various jurisdictions, including the United States, to our international

business activities, changes in tax rates, new or revised tax laws or interpretations of existing tax laws and policies, and its ability to operate our business in a manner consistent with its corporate structure and intercompany arrangements. The relevant taxing authorities may disagree with our determinations as to the income and expenses attributable to specific jurisdictions. If such a disagreement were to occur, and our position was not sustained, we could be required to pay additional taxes, interest and penalties, which could result in one-time tax charges, higher effective tax rates, reduced cash flows and lower overall profitability of its operations.

We will be subject to U.S. federal, state, and local income, sales, and other taxes in the United States and income, withholding, transaction, and other taxes in numerous foreign jurisdictions. Significant judgment will be required in evaluating its tax positions and its worldwide provision for taxes. During the ordinary course of our business, there are many activities and transactions for which the ultimate tax determination may be uncertain. In addition, its tax obligations and effective tax rates could be adversely affected by changes in the relevant tax, accounting and other laws, regulations, principles and interpretations, including those relating to income tax nexus, by recognizing tax losses or lower than anticipated earnings in jurisdictions where it has lower statutory rates and higher than anticipated earnings in jurisdictions where it has higher statutory rates, by changes in foreign currency exchange rates, or by changes in the valuation of its deferred tax assets and liabilities. We may be audited in various jurisdictions, and such jurisdictions may assess additional taxes, sales taxes and value added taxes against it. Even if we believe our tax estimates are reasonable, the final determination of any tax audits or litigation could be materially different from our historical tax provisions and accruals, which could have an adverse effect on our results of operations or cash flows in the period or periods for which a determination is made.

If our estimates or judgments relating to its critical accounting policies prove to be incorrect or financial reporting standards or interpretations change, our results of operations could be adversely affected.

The preparation of financial statements in conformity with GAAP requires management to make estimates and assumptions that affect the amounts reported in our consolidated financial statements and accompanying notes. We have historically based our estimates on historical experience and on various other assumptions that we believe to be reasonable under the circumstances, as discussed in the section titled “Management’s Discussion and Analysis of Financial Condition and Results of Operations.” The results of these estimates form the basis for making judgments about the carrying values of assets, liabilities and equity, and the amount of revenue and expenses that are not readily apparent from other sources. Significant assumptions and estimates used in preparing our consolidated financial statements will include, and may include in the future, those related to revenue recognition; allowance for doubtful accounts; costs to obtain or fulfill a contract; valuation of common stock; valuation of stock-based compensation; carrying value and useful lives of long-lived assets; loss contingencies; and the provision for income our and related deferred taxes. Our results of operations may be adversely affected if its assumptions change or if actual circumstances differ from those in our assumptions, which could cause our results of operations to fall below the expectations of industry or financial analysts and investors, resulting in a decline in the market price of the common stock.

Additionally, we will regularly monitor our compliance with applicable financial reporting standards and review new pronouncements and drafts thereof that are relevant to us. As a result of new standards, changes to existing standards and changes in their interpretation, we might be required to change our accounting policies, alter our operational policies and implement new or enhance existing systems so that they reflect new or amended financial reporting standards, or we may be required to restate our published financial statements. Such changes to existing standards or changes in their interpretation may have an adverse effect on our reputation, business, financial position and profit, or cause an adverse deviation from our revenue and operating profit targets, which may negatively impact our financial results.

Our business will be subject to the risks of natural catastrophic events and to interruption by man-made problems such as power disruptions, computer viruses, data security breaches or terrorism.

A significant natural disaster, such as an earthquake, a fire, a flood, or significant power outage could have a material adverse impact on our business, results of operations and financial condition. Natural disasters could affect our personnel, data centers, supply chain, manufacturing vendors, or logistics providers' ability to provide materials and perform services such as manufacturing products or assisting with shipments on a timely basis. In addition, climate change could result in an increase in the frequency or severity of natural disasters. In the event that we or our service providers' information technology systems or manufacturing or logistics abilities are hindered by any of the events discussed above, we could result in missed financial targets, such as revenue, for a particular quarter. In addition, computer malware, viruses and computer hacking, fraudulent use attempts and phishing attacks have become more prevalent in the cybersecurity industry, and our internal systems may be victimized by such attacks. Likewise, we could be subject to other man-made problems, including but not limited to power disruptions and terrorist acts.

Although we will maintain incident management and disaster response plans, in the event of a major disruption caused by a natural disaster or man-made problem, we may be unable to continue its operations and may endure system interruptions, reputational harm, delays in our development activities, lengthy interruptions in service, breaches of data security and loss of critical data, and our insurance may not cover such events or may be insufficient to compensate it for the potentially significant losses we may incur. Acts of terrorism and other geo-political unrest could also cause disruptions in our business or the business of our supply chain, manufacturers, logistics providers, partners, or customers or the economy as a whole. Any disruption in the business of its supply chain, manufacturers, logistics providers, partners or customers that impacts sales at the end of a fiscal quarter could have a significant adverse impact on our financial results. All of the aforementioned risks may be further increased if disaster recovery plans prove to be inadequate. To the extent that any of the above should result in delays or cancellations of customer orders, or the delay in the manufacture, deployment, or shipment of our products, our business, financial condition, and results of operations would be adversely affected.

Our management identified material weaknesses in its internal control over financial reporting and may identify additional material weaknesses in the future or otherwise fail to maintain effective internal control over financial reporting, which may result in material misstatements of our financial statements or cause us to fail to meet our periodic reporting obligations.

In connection with the preparation and audit of our consolidated financial statements for the year ended January 31, 2021, we and our independent registered public accounting firm identified material weaknesses in our internal control over financial reporting. A material weakness is a deficiency, or a combination of deficiencies, in internal control over financial reporting such that there is a reasonable possibility that a material misstatement of our annual or interim financial statements will not be prevented or detected on a timely basis. We did not have a sufficient number of personnel with an appropriate degree of accounting and internal controls knowledge, experience, and training to appropriately analyze, record and disclose accounting matters commensurate with our accounting and reporting requirements, which resulted in an inability to consistently establish appropriate authorities and responsibilities in pursuit of its financial reporting objectives. This material weakness contributed to the following additional material weaknesses: we did not design and maintain effective controls over the review of journal entries and account reconciliations. Specifically, certain personnel have the ability to both (i) create and post journal entries within our general ledger system, and (ii) prepare and review account reconciliations. we did not design and maintain effective controls over information technology ("**IT**") general controls for information systems that are relevant to the preparation of our financial statements. Specifically, we did not design and maintain: (i) program change management controls for the financial systems to ensure that information technology program and data changes affecting financial IT applications and underlying accounting records are identified, tested, authorized and implemented appropriately; (ii) appropriate user access controls to ensure appropriate segregation of duties and that adequately restrict user and privileged

access to financial applications, programs and data to appropriate personnel; (iii) computer operations controls to ensure data backups are authorized and restorations monitored; and (iv) testing and approval controls for program development to ensure that new software development is aligned with business and IT requirements.

These material weaknesses did not result in a material misstatement to the consolidated financial statements. However, these material weaknesses could result in a misstatement of substantially all accounts or disclosures that would result in a material misstatement to the annual or interim consolidated financial statements that would not be prevented or detected.

With the oversight of senior management, we have instituted and continue to execute on plans to remediate these material weaknesses and will continue to take remediation steps, including hiring additional key supporting accounting personnel with public company reporting and accounting operations experience, implementing the required segregation of roles and duties both in manual and systems related processes including for journal entries and account reconciliations, and formalizing the documentation and performance of information technology general controls for information systems utilized for financial reporting.

While we implement and execute on our plan to remediate the material weaknesses described above, we cannot predict the success of such plans or the outcome of our assessment of these plans at this time. If the steps are insufficient to remediate the material weaknesses successfully and otherwise establish and maintain effective internal control over financial reporting, the reliability of our financial reporting, investor confidence, and the value of our common stock could be materially and adversely affected. We can give no assurance that the implementation of this plan will remediate these deficiencies in our internal control over financial reporting or that additional material weaknesses or significant deficiencies in our internal control over financial reporting will not be identified in the future. The failure to implement and maintain effective internal control over financial reporting could result in errors in its financial statements that could result in a restatement of our financial statements, causing us to fail to meet our reporting obligations.

Risks Related to an Investment in Our Securities

There may not be an active trading market for our common stock, which may make it difficult to sell shares of our common stock.

It is possible that an active trading market will not develop or, if developed, that any market will not be sustained. This would make it difficult for you to sell shares of our common stock at an attractive price or at all.

The market price of shares of our common stock may be volatile, which could cause the value of your investment to decline.

The market price of our common stock may be highly volatile and could be subject to wide fluctuations. Securities markets worldwide experience significant price and volume fluctuations. The securities markets have experienced significant volatility as a result of the COVID-19 pandemic. Market volatility, as well as general economic, market or political conditions, could reduce the market price of shares of our common stock regardless of our operating performance. Our operating results could be below the expectations of public market analysts and investors due to a number of potential factors, including:

- variations in quarterly operating results or dividends, if any, to stockholders;
- additions or departures of key management personnel;
- publication of research reports about our industry;
- litigation and government investigations;
- changes or proposed changes in laws or regulations or differing interpretations or enforcement of laws or regulations affecting our business;
- adverse market reaction to any indebtedness incurred or securities issued in the future;

- changes in market valuations of similar companies;
- adverse publicity or speculation in the press or investment community;
- announcements by competitors of significant contracts, acquisitions, dispositions, strategic partnerships, joint ventures, or capital commitments; and
- the impact of the COVID-19 pandemic (or future pandemics) on our management, employees, partners, customers, and operating results.

In response to any of the foregoing developments, the market price of shares of our common stock could decrease significantly. You may be unable to resell your shares at or above your purchase price.

In addition, price volatility may be greater if the public float and trading volume of our common stock is low. For example, the trading price of our common stock following the consummation of the Business Combination has been extremely volatile, ranging between $10.84 and $47.50 per share, and has fluctuated in response to various factors, some of which are beyond our control, and this volatility could be accentuated by the limited public float of our shares relative to our overall capitalization.

Following periods of volatility in the overall market and the market price of a company's securities, securities class action litigation has often been instituted against that company. Any such litigation, if instituted against us, could result in substantial costs and a diversion of management's attention and resources.

A small number of stockholders will continue to have substantial control over us, which may limit other stockholders' ability to influence corporate matters and delay or prevent a third party from acquiring control over us.

Our directors and executive officers and beneficial owners of 5% or more of our voting securities and their respective affiliates, beneficially owned, in the aggregate, approximately 43% of our outstanding common stock as of the closing of the Business Combination. This significant concentration of ownership may have a negative impact on the trading price for our common stock because investors often perceive disadvantages in owning stock in companies with controlling stockholders. In addition, these stockholders will be able to exercise influence over all matters requiring stockholder approval, including the election of directors and approval of corporate transactions, such as a merger or other sale of our company or our assets. This concentration of ownership could limit stockholders' ability to influence corporate matters and may have the effect of delaying or preventing a change in control, including a merger, consolidation or other business combination, or discouraging a potential acquirer from making a tender offer or otherwise attempting to obtain control, even if that change in control would benefit the other stockholders.

There can be no assurance that we will be able to comply with the continued listing standards of the NYSE.

If NYSE delists our securities from trading on its exchange for failure to meet the listing standards, we and our stockholders could face significant negative consequences including:

- limited availability of market quotations for our securities;
- a determination that our common stock is a "penny stock" which will require brokers trading in our common stock to adhere to more stringent rules,
- possibly resulting in a reduced level of trading activity in the secondary trading market for shares of our common stock;
- a limited amount of analyst coverage; and
- a decreased ability to issue additional securities or obtain additional financing in the future.

If our operating and financial performance in any given period does not meet the guidance provided to the public or the expectations of investment analysts, the market price of our common stock may decline.

We may, but are not obligated to, provide public guidance on our expected operating and financial results for future periods. Any such guidance will consist of forward-looking statements, subject to the risks and uncertainties described in this prospectus and in our other public filings and public statements. The ability to provide this public guidance, and the ability to accurately forecast our results of operations, could be impacted by the COVID-19 pandemic. Our actual results may not always be in line with or exceed any guidance it has provided, especially in times of economic uncertainty, such as the current global economic uncertainty being experienced as a result of the COVID-19 pandemic. If, in the future, our operating or financial results for a particular period do not meet any guidance provided or the expectations of investment analysts, or if we reduce our guidance for future periods, the market price of our common stock may decline as well. Even if we do issue public guidance, there can be no assurance that we will continue to do so in the future.

We qualify as an "emerging growth company." The reduced public company reporting requirements applicable to emerging growth companies may make our common stock less attractive to investors.

We qualify as an "emerging growth company" under SEC rules. As an emerging growth company, we are permitted and plan to rely on exemptions from certain disclosure requirements that are applicable to other public companies that are not emerging growth companies. These provisions include, but are not limited to: (1) an exemption from compliance with the auditor attestation requirement in the assessment of internal control over financial reporting pursuant to Section 404 of Sarbanes-Oxley, (2) not being required to comply with any requirement that may be adopted by the PCAOB regarding mandatory audit firm rotation or a supplement to the auditor's report providing additional information about the audit and the financial statements, (3) reduced disclosure obligations regarding executive compensation arrangements in periodic reports, registration statements, and proxy statements, and (4) exemptions from the requirements of holding a nonbinding advisory vote on executive compensation and stockholder approval of any golden parachute payments not previously approved. Further, Section 102(b)(1) of the JOBS Act exempts emerging growth companies from being required to comply with new or revised financial accounting standards until private companies (that is, those that have not had a Securities Act registration statement declared effective or do not have a class of securities registered under the Exchange Act) are required to comply with the new or revised financial accounting standards. The JOBS Act provides that a company can elect to opt out of the extended transition period and comply with the requirements that apply to non-emerging growth companies but any such election to opt out is irrevocable. As a result, the information we provide will be different than the information that is available with respect to other public companies that are not emerging growth companies. If some investors find our common stock less attractive as a result, there may be a less active trading market for our common stock, and the market price of our common stock may be more volatile.

Our management has limited experience in operating a public company.

Our executive officers have limited experience in the management of a publicly traded company. Our management team may not successfully or effectively manage our transition to a public company that will be subject to significant regulatory oversight and reporting obligations under federal securities laws. Our limited experience in dealing with the increasingly complex laws pertaining to public companies could be a significant disadvantage in that we are likely that an increasing amount of their time may be devoted to these activities, which will result in less time being devoted to the management and our growth. We may not have adequate personnel with the appropriate level of knowledge, experience, and training in the accounting policies, practices or internal control over financial reporting required of public companies in the United States. The development and implementation of the standards and controls necessary for us to achieve the level of accounting standards required of a public company in the United States may require costs greater than expected. It is possible that we will be required to expand its employee base and hire additional employees to support its operations as a public company, which will increase its operating costs in future periods.

Customer retention

Our ability to increase revenue depends in large part on our ability to retain existing customers.

Investing in business growth

Since inception, we have invested significantly in the growth of our business. We intend to continue to invest in our research and development team to lead product improvements, our sales team to broaden our brand awareness and our general and administrative expenses to increase for the foreseeable future given the additional expenses for finance, compliance and investor relations as we grow as a public company. In addition to our internal growth, we may also consider acquisitions of businesses, technologies, and assets that complement and bolster additional capabilities to our product offerings.

Key Business Metrics

We monitor the following key metrics to measure our performance, identify trends, formulate business plans and make strategic decisions.

Recurring Software Customers

We believe that our ability to increase the number of subscription and other recurring contract type customers on our platform is an indicator of our market penetration, the growth of our business, and our potential future business opportunities. We have a history of growing the number of customers who have contracted for our platforms on a recurring basis, which does not include our professional services customers. Our recurring software customers include customers who have a recurring contract for either or both of our IronDefense and IronDome platforms. These platforms are generally sold together, but they also can be purchased on a standalone basis. We have consistently increased the number of such customers period-over-period, and we expect this trend to continue as we increase subscription offerings to small and medium-sized businesses, in addition to increased subscription offerings for our larger enterprise customers. The following table sets forth the number of recurring software customers as of the dates presented:

	July 31,	
	2021	2020
Recurring Software Customers	51	22
Year-over-year growth	132%	22%
	January 31,	
	2021	2020
Recurring Software Customers	27	20
Year-over-year growth	35%	43%

Annual Recurring Revenue ("ARR")

ARR is calculated at a particular measurement date as the annualized value of our then existing customer subscription contracts and the portions of other software and product contracts that are to be recognized over the course of the contracts and that are designed to renew, assuming any contract that expires during the 12 months following the measurement date is renewed on its existing terms. We believe this is a reasonable assumption as less than 1% of an approximate total of $160 million in cumulative ARR that would have been reported over the last 12 quarters through the end of fiscal year 2021 did not renew their contract. The following table sets forth our ARR as of the dates presented:

	July 31,	
	2021	2020
	(in millions)	
Annual recurring revenues	$24.1	$19.5
Year-over-year growth	24%	21%

	January 31,	
	2021	2020
	(in millions)	
Annual recurring revenues	$25.8	$15.0
Year-over-year growth	72%	37%

Dollar-based Average Contract Length

Our dollar-based average contract length is calculated from a set of customers against the same metric as of a prior period end. Because many of our customers have similar buying patterns and the average term of our contracts is more than 12 months, this metric provides a means of assessing the degree of built-in revenue repetition that exists across our customer base.

We calculate our dollar-based average contract length as follows:

- Numerator: We multiply the average total length of the contracts, measured in years or fractions thereof, by the respective revenue recognized for the last six months of each reporting period.
- Denominator: We use the revenue attributable to software and product customers for the same six month period used in the numerator. This effectively represents the revenue base that is being generated by those customers.

Dollar-based average contract length is obtained by dividing the Numerator by the Denominator. Our dollar-based average contract length decreased from 3.2 to 2.8 years, or (13)%, for the six months ended July 31, 2021 as compared to the six months ended July 31, 2020, and decreased from 3.5 to 2.9 years, or 17% for the year ended January 31, 2021 as compared to the year ended January 31, 2020. As our revenues and our customer base increases, we expect our average contract length to trend downward over time. Declines in average contract length are not reflective of the average lifetime of a customer.

	July 31,	
	2021	2020
	(in years)	
Dollar-based average contract length	2.8	3.2

	January 31,	
	2021	2020
	(in years)	
Dollar-based average contract length	2.9	3.5

Calculated Billings

Calculated billings is a non-GAAP financial measure that we believe is a key metric to measure our periodic performance. Calculated billings represent our total revenue plus the change in deferred revenue in a period. Calculated billings in any particular period aims to reflect amounts invoiced to customers to access our software-based, cybersecurity analytics products, cloud platform and professional services, together with related support services, for our new and existing customers. We typically invoice our customers on multi-year or annual contracts in advance, either annually or monthly. Calculated billings decreased $4.3 million, or (26)%, in year to date 2022 over year to date 2021 and increased $19.7 million, or 85%, in fiscal 2021 over fiscal 2020. Calculated billings decreased when comparing year to date 2022 to year to date 2021 primarily due to lower revenue and during fiscal year 2021, IronNet was focused on growing their deferred revenue. As deferred revenue remains more consistent, we expect our calculated billings growth rate to trend down over time. We also expect that calculated billings will be affected by timing of entering into agreements with customers; and the mix of billings in each reporting period as we typically invoice customers multi-year or annually in advance and, to a lesser extent, monthly in advance.

While we believe that calculated billings may be helpful to investors because it provides insight into the cash that will be generated from sales of our subscriptions, this metric may vary from period-to-period for a number of reasons, and therefore has a number of limitations as a quarter-to-quarter or year-over-year comparative measure. In addition, other companies, including companies in our industry, may calculate similarly-titled non-GAAP measures differently or may use other measures to evaluate their performance, all of which could reduce the usefulness of our metric of calculated billings as tools for comparison. Because of these and other limitations, you should consider calculated billings along with revenue and our other GAAP financial results.

The following table presents a reconciliation of revenue, the most directly comparable financial measure calculated in accordance with GAAP, to calculated billings:

	Six Months Ended July 31,			
	2021	2020	2021 vs 2020	
	(in millions)			
Revenue	$12.5	$14.8	(2.3)	(16)%
Add: Total Deferred revenue, end of period	33.6	21.9	11.7	53
Less: Total Deferred revenue, beginning of period	34.0	20.3	13.7	67
Calculated billings	$12.1	$16.4	$(4.3)	(26)%

	Year Ended January 31,			
	2021	2020	2021 vs 2020	
	(in millions)			
Revenue	$29.2	$23.2	6.1	26%
Add: Total Deferred revenue, end of period	34.0	20.3	13.7	67
Less: Total Deferred revenue, beginning of period	20.3	20.3	0.0	0
Calculated billings	$42.9	$23.2	$ 19.7	85%

Components of Our Results of Operations

Revenue

Our revenues are derived from sales of software subscriptions, subscription-like software products and software support contracts as well as from professional services. Products, subscriptions and support revenues accounted for 95% of our revenue in quarter to date 2022, for 84% of our revenue in quarter to date 2021, for 96% of our revenue in year to date 2022, for 82% of our revenue in year to date 2021, and for 85% of our

revenue for each of fiscal 2021 and fiscal 2020. Professional services revenues accounted for 5% of our revenue in quarter to date 2022, for 16% of our revenue in our quarter to date 2021, for 4% of our revenue in year to date 2022, for 18% of our revenue in year to date 2021 and for 15% of our revenue for each of fiscal 2021 and fiscal 2020.

Our typical customer contracts and subscriptions range from one to five years. We typically invoice customers in advance. We combine intelligence dependent hardware and software licenses as well as subscription-type deliverables with the related threat intelligence and support and maintenance as a single performance obligation, as it delivers the essential functionality of our cybersecurity solution. Most companies also participate in the IronDome collective defense software solution that provides them access to IronNet's collective defense infrastructure linking participating stakeholders. As a result, we recognize revenue for this single performance obligation ratably over the expected term with the customer. Amounts that have been invoiced are recorded in deferred revenue or they are recorded in revenue if the revenue recognition criteria have been met. Significant judgement is required for the assessment of material rights relating to renewal options associated with our contracts.

Professional services revenues are generally sold separately from our products and include services such as development of national cyber security strategies, cyber operations monitoring, security, training, red team, incident response and tailored maturity assessments. Revenue derived from these services is recognized as the services are delivered.

Cost of Revenue

Cost of product, subscription and support revenue includes expenses related to our hosted security software, employee-related costs of our customer facing support, such as salaries, bonuses and benefits, an allocated portion of administrative costs and the amortization of deferred costs.

Cost of professional services revenue consists primarily of employee-related costs, such as salaries, bonuses and benefits, cost of contractors and an allocated portion of administrative costs.

Gross Profit

Gross profit, calculated as total revenue less total costs of revenue is affected by various factors, including the timing of our acquisition of new customers, renewals from existing customers, the data center and bandwidth costs associated with operating our cloud platform, the extent to which we expand our customer support organization, and the extent to which we can increase the efficiency of our technology and infrastructure through technological improvements. Also, we view our professional services in the context of our larger business and as a significant lead generator for future product sales. Because of these factors, our services revenue and gross profit may fluctuate over time.

Operating Expenses

Research and development

Our research and development efforts are aimed at continuing to develop and refine our products, including adding new features and modules, increasing their functionality, and enhancing the usability of our platform. Research and development costs primarily include personnel-related costs and acquired software costs. Research and development costs are expensed as incurred.

Sales and marketing

Sales and marketing expenses consist primarily of employee compensation and related expenses, including salaries, bonuses and benefits for our sales and marketing employees, sales commissions that are recognized as

expenses over the period of benefit, marketing programs, travel and entertainment expenses, and allocated overhead costs. We capitalize our sales commissions and recognize them as expenses over the estimated period of benefit.

We intend to continue to make significant investments in our sales and marketing organization to drive additional revenue, further penetrate the market and expand our global customer base. In particular, we will continue to invest in growing and training our sales force, broadening our brand awareness and expanding and deepening our channel partner relationships. We expect our sales and marketing expenses to decrease as a percentage of our revenue over the long term, although our sales and marketing expenses may fluctuate as a percentage of our revenue from period to period due to the timing and extent of these expenses.

General and administrative

General and administrative costs include salaries, stock-based compensation expenses, and benefits for personnel involved in our executive, finance, legal, people and culture, and administrative functions, as well as third-party professional services and fees, and overhead expenses.

We expect that general and administrative expenses will increase in absolute dollars as we hire additional personnel and enhance our systems, processes, and controls to support the growth in our business as well as our increased compliance and reporting requirements as a public company.

Other income (expense), net

Other income (expense), net consists primarily of interest income, interest expense, and foreign currency exchange gains and losses.

Provision for income taxes

Provision for income taxes consists of federal and state income taxes in the United States and income taxes and withholding taxes in certain foreign jurisdictions in which we conduct business. We maintain a full valuation allowance on our U.S. federal and state deferred tax assets.

Results of Operations

Comparison of Quarter to Date 2022 and Quarter to Date 2021

The following tables set forth our consolidated statement of operations in dollar amounts and as a percentage of total revenue for each period presented (dollars in millions):

	Three Months Ended July 31,					
	2021		2020		2021 vs 2020	
	(in millions)					
Software, subscription and support revenue	$ 5.8	95%	$ 6.7	84%	$(0.9)	-14%
Professional services revenue	0.3	5%	1.2	16%	(0.9)	-75%
Total revenue	6.1	100%	7.9	100%	(1.9)	-24%
Cost of software, subscription and support revenue	1.7	27%	1.1	14%	0.6	53%
Cost of professional service revenue	0.1	2%	0.1	2%	0.0	20%
Total cost of revenue	1.8	30%	1.2	15%	0.6	50%
Gross profit	4.3	70%	6.7	85%	(2.5)	-37%
Operating expenses:						
Research and development	7.6	125%	6.9	86%	0.7	10%
Sales and marketing	7.7	127%	7.9	99%	(0.2)	-3%
General and administrative	6.0	98%	6.2	78%	(0.2)	-3%
Total operating expenses	21.2	349%	20.9	263%	0.3	1%
Operating loss	(17.0)	-279%	(14.2)	-179%	(2.8)	20%
Other (expense) income, net	(0.2)	-4%	(0.1)	-1%	(0.2)	208%
Loss before provision for income taxes	(17.2)	-283%	(14.3)	-180%	(2.9)	21%
Provision for income taxes	0.0	1%	(0.0)	0%	0.1	nm
Net loss	$(17.2)	-283%	$(14.3)	-180%	$(2.9)	20%

Nm – Not meaningful

Revenue

Total revenue decreased by $1.9 million or (24)% in quarter to date 2022 compared to quarter to date 2021.

Software revenue decreased by $0.9 million or (14)% primarily due to the Company's transition from contracts that had material non-recurring elements which would not renew in full to contract forms that were designed to fully renew. Therefore, the non-recurring revenue elements of contracts were minimized.

Despite the overall decline in software, subscription and support revenue, the subscription revenue portion increased by $0.5 million or 9%, in quarter to date 2022, from $5.3 million to $5.8 million and accounted for 100% of our total software revenue in quarter to date 2022, up from 79% in quarter to date 2021. A majority of that growth compared to the same period of last year has come from new customers in the Asia-Pacific region. New customers, worldwide, accounted for $2.3 million of the subscription revenue quarter to date 2022.

Professional services revenue decreased $0.9 million or (75)% in quarter to date 2022 compared to quarter to date 2021, primarily due to the completion of a national cybersecurity strategy engagement in EMEA in fiscal 2021 and delays in professional services contract starts in quarter to date 2022 due to lockdowns from COVID-19, which are expected in the second half of fiscal year 2022. Professional services accounted for 5% of our total revenue in quarter to date 2022 and for 16% of our total revenue in quarter to date 2021.

Cost of revenue

Total cost of revenue increased by $0.6 million or 50%, in quarter to date 2022, compared to quarter to date 2021. Cost of software, subscription and support revenue increased by $0.6 million or 53%, in quarter to date

2022, compared to quarter to date 2021. The increase was due primarily to an increase in customer cloud cost during quarter to date 2022 compared to quarter to date 2021.

Cost of professional service revenue remained consistent when comparing quarter to date 2022 and quarter to date 2021.

Gross Profit and Gross Margin

Mix changes in cost of revenue resulted in a decrease in software gross margin to 71.1% in quarter to date 2022 compared to 83.7% in quarter to date 2021, and a decrease in professional services gross margin to 52.0% in quarter to date 2022 compared to 90.1% in quarter to date 2021. Quarter to date 2021 margin was unusually high as we onboarded 2 significant revenue customers which hadn't yet ramped their full cloud costs in period and finalized delivery of key significant service contract in EMEA. Professional services margin will continue to be volatile contract to contract as we scale the business.

We expect that gross margins for the rest of fiscal 2022 to improve slightly to achieve our full year guidance. Margins may remain volatile compared to fiscal 2021 due to the continuing presence of large contracts in our revenue mix.

The following tables show gross profit and gross margin, respectively, for software products and support revenue and professional services revenue for quarter to date 2022 as compared to quarter to date 2021.

	Three Months Ended July 31,			
	2021	2020	2021 vs 2020	
	(in millions)			
Software products margin	$ 4.1	$ 5.6	$ (1.5)	-27%
Professional services margin	0.2	1.1	(1.0)	-86%
Total Gross profit margin	$ 4.3	$ 6.7	$ (2.5)	-37%

	2021	2020	Change
Software products margin	71.1%	83.7%	-12.6%
Professional services margin	52.0%	90.1%	-38.2%
Total Gross profit margin	70.1%	84.7%	-14.6%

Operating expenses

Research and development

Research and development expenses increased by $0.7 million or 10%, in quarter to date 2022, compared to quarter to date 2021 primarily due to the ramping resources to support product development. At 125% of total revenues in quarter to date 2022 compared to 86% in quarter to date 2021, we expect that our overall R&D expenditure rate as a percentage of revenues will decline in the future.

Sales and marketing

Sales and marketing cost decreased by $0.2 million or (3)% in quarter to date 2022, compared to quarter to date 2021, primarily due to a large number of newly hired but not yet trained sales and marketing personnel in quarter to date 2021 which, decreased 20% over the course of the fiscal year as the company settled on its highest performing personnel. This led to an 8% decrease in sales and marketing payroll costs in year to date 2022 compared to the comparable period prior year. At 127% of total revenues in quarter to date 2022 compared to 99% in quarter to date 2021, we expect that our overall sales and marketing expenditure rates as a percentage of revenues will decline in the future.

General and administrative

General and administrative costs decreased by $0.2 million when comparing quarter to date 2022 to quarter to date 2021, quarter to date 2022 includes $0.6 million of one-time charges relating to the Business Combination. Quarter to date 2022 general and administrative expenses were at 98% of total revenues compared to 78% in quarter to date 2021. Quarter to date 2022 expenses were higher due to additional costs stemming from preparations to operate as an SEC compliant company and a lower-than-normal building rent, travel and depreciation expenses during quarter to date 2021 as the company was operating in a wholly remote manner. We expect that our overall general and administrative expenditure rates as a percentage of revenues will decline in the future.

Other (expense) income, net

Other (expense) income, changed by $(0.2) million in quarter to date 2022, compared to quarter to date 2021, primarily due to an increase in interest expense related to the new loan entered into during the three months ended July 31, 2021. Please refer to the Liquidity and Capital Resources section for more information about the loan.

Provision for income taxes

The change in provision for income taxes was immaterial to the results of operations primarily due to our continued net loss position, the accumulation of net loss carryforwards, and offsetting valuation allowance.

Comparison of Year to Date 2022 and Year to Date 2021

The following tables set forth our consolidated statements of operations in dollar amounts and as a percentage of total revenue for each period presented (dollars in millions):

	Six Months Ended July 31,				2021 vs 2020	
	2021		2020			
	(in millions)					
Software, subscription and support revenue	$ 11.9	96%	$ 12.1	82%	$(0.2)	-2%
Professional services revenue	0.5	4%	2.7	18%	(2.2)	-80%
Total revenue	12.5	100%	14.8	100%	(2.4)	-16%
Cost of software, subscription and support revenue	3.4	27%	2.6	18%	0.8	30%
Cost of professional service revenue	0.3	3%	0.4	3%	(0.1)	-24%
Total cost of revenue	3.8	30%	3.1	21%	0.7	23%
Gross profit	8.7	70%	11.8	79%	(3.1)	-26%
Operating expenses:						
Research and development	14.5	116%	14.3	96%	0.2	1%
Sales and marketing	14.8	119%	16.1	109%	(1.3)	-8%
General and administrative	11.7	94%	12.0	81%	(0.3)	-2%
Total operating expenses	41.0	329%	42.4	286%	(1.4)	-3%
Operating loss	(32.3)	-259%	(30.6)	-207%	(1.7)	5%
Other (expense) income, net	(0.4)	-3%	(0.1)	0%	(0.3)	581%
Loss before provision for income taxes	(32.6)	-262%	(30.7)	-207%	(2.0)	6%
Provision for income taxes	(0.0)	0%	(0.0)	0%	0.0	nm
Net loss	$(32.7)	-262%	$(30.7)	-207%	$(2.0)	6%

Nm – Not meaningful

Revenue

Total revenue decreased by $2.4 million or (16)% in year to date 2022 compared to year to date 2021.

Software revenue decreased by $0.2 million primarily due to the Company's transition from contracts that had material non-recurring elements which would not renew in full to contract forms that were designed to fully renew. Therefore, the non-recurring revenue elements of contracts were minimized.

Despite the overall decline in software, subscription and support revenue, the subscription revenue portion increased by $2.8 million or 31%, in year to date 2022, from $9.1 million to $11.9 million and accounted for 100% of our total software revenue in year to date 2022, up from 75% in year to date 2021. A majority of that growth compared to the same period of last year has come from the Asia-Pacific region. New customers, worldwide, accounted for $4.6 million of the subscription revenue year to date 2022.

Professional services revenue decreased $2.2 million or (80)% in year to date 2022 compared to year to date 2021, primarily due to the completion of a national cybersecurity strategy engagement in EMEA in fiscal 2021 and delays in professional services contract starts in year to date 2022 due to lockdowns from COVID-19, which are expected in the second half of fiscal year 2022. Professional services accounted for 4% of our total revenue in year to date 2022 and for 18% of our total revenue in year to date 2021.

Cost of revenue

Total cost of revenue increased by $0.7 million or 23%, in year to date 2022, compared to year to date 2021. Cost of software, subscription and support revenue increased by $0.8 million or 30%, in year to date 2022, compared to year to date 2021. The increase was due primarily to an increase in customer cloud cost during year to date 2022 compared to year to date 2021.

Cost of professional service revenue decreased by $0.1 million or (24)% in year to date 2022, compared to year to date 2021. The decrease in cost of service revenue was primarily due to a decrease in overall professional services activity in year to date 2022 compared to year to date 2021.

Gross Profit and Gross Margin

Mix changes in cost of revenue resulted in a decrease in software gross margin to 71.3% in year to date 2022 compared to 78.3% in year to date 2021, and a decrease in professional services gross margin to 39.4% in year to date 2022 compared to 84.0% in year to date 2021. Year to date 2021 margin was unusually high as we onboarded 2 significant revenue customers which hadn't yet ramped their full cloud costs in period and finalized delivery of key significant service contract in EMEA. Professional services margin will continue to be volatile contract to contract as we scale the business.

We expect that gross margins for the rest of fiscal 2022 to improve. Margins may remain volatile compared to fiscal 2021 due to the continuing presence of large contracts in our revenue mix.

The following tables show gross profit and gross margin, respectively, for software products and support revenue and professional services revenue for year to date 2022 as compared to year to date 2021.

	Six Months Ended July 31,			
	2021	2020	2021 vs 2020	
	(in millions)			
Software products margin	$ 8.5	$ 9.5	$ (1.0)	-10%
Professional services margin	0.2	2.3	(2.1)	-91%
Total Gross profit margin	$ 8.7	$11.8	$ (3.1)	-26%

	2021	2020	Change
Software products margin	71.3%	78.3%	-7.0%
Professional services margin	39.4%	84.0%	-44.6%
Total Gross profit margin	69.9%	79.3%	-9.5%

Operating expenses

Research and development

Research and development expenses increased by $0.2 million or 1%, in year to date 2022, compared to year to date 2021 primarily due to the ramping resources to support product development. At 116% of total revenues in year to date 2022 compared to 96% in year to date 2021, we expect that our overall R&D expenditure rate as a percentage of revenues will decline in the future.

Sales and marketing

Sales and marketing cost decreased by $1.3 million or (8)% in year to date 2022, compared to year to date 2021, primarily due to a large number of newly hired but not yet trained sales and marketing personnel in year to date 2021 which, decreased 20% over the course of the fiscal year as the company settled on its highest performing personnel. This led to an 8% decrease in sales and marketing payroll costs in year to date 2022 compared to the comparable period prior year. At 119% of total revenues in year to date 2022 compared to 109% in year to date 2021, we expect that our overall sales and marketing expenditure rates as a percentage of revenues will decline in the future.

General and administrative

General and administrative costs decreased by $0.3 million when comparing year to date 2022 to year to date 2021, year to date 2022 includes $0.6 million of one-time charges relating to the Business Combination. Year to date 2022 general and administrative expenses were at 94% of total revenues compared to 81% in year to date 2021. Year to date 2022 expenses were higher due to additional costs stemming from preparations to operate as an SEC compliant company and a lower-than-normal building rent, travel and depreciation expenses during year to date 2021 as the company was operating in a wholly remote manner. We expect that our overall general and administrative expenditure rates as a percentage of revenues will decline in the future.

Other (expense) income, net

Other (expense) income, changed by $(0.3) million in year to date 2022, compared to year to date 2021, primarily due to an increase in interest expense related to the new loan entered into during the three months ended July 31, 2021. Please refer to the Liquidity and Capital Resources section for more information about the loan.

Provision for income taxes

The change in provision for income taxes was immaterial to the results of operations primarily due to our continued net loss position, the accumulation of net loss carryforwards, and offsetting valuation allowance.

Comparison of Fiscal 2021 and Fiscal 2020

The following tables set forth our consolidated statements of operations in dollar amounts and as a percentage of total revenue for each period presented (dollars in millions):

	Year Ended January 31,					
	2021		2020		2021 vs 2020	
	(in millions)					
Products, subscription and support revenue	$ 24.7	85%	$ 19.8	85%	$ 4.9	25%
Professional services revenue	4.5	15%	3.4	15%	1.1	32%
Total revenue	29.2	100%	23.2	100%	6.0	26%
Cost of product, subscription and support revenue	5.4	18%	5.9	25%	(0.5)	-8%
Cost of professional service revenue	1.6	5%	0.7	3%	0.9	129%
Total cost of revenue	7.0	24%	6.6	29%	0.4	6%
Gross profit	22.2	76%	16.6	72%	5.6	34%
Operating expenses:						
Research and development	25.8	88%	26.6	115%	(0.8)	-3%
Sales and marketing	30.4	104%	17.9	77%	12.5	70%
General and administrative	21.3	73%	20.5	88%	0.8	4%
Total operating expenses	77.5	265%	65.0	280%	12.5	19%
Operating loss	(55.3)	-189%	(48.4)	-209%	(6.9)	14%
Other income, net	(0.0)	0%	0.5	2%	(0.5)	-100%
Loss before provision for income taxes	(55.3)	-189%	(47.9)	-206%	(7.4)	15%
Provision for income taxes	(0.1)	0%	(0.0)	0%	(0.1)	nm
Net loss	$ (55.4)	-190%	$ (47.9)	-206%	$ (7.5)	16%

Nm – not meaningful

Revenue

Total revenue increased by $6.0 million or 26% in fiscal 2021 compared to fiscal 2020. The increase was mostly due to disproportionally high growth as the APJ and EMEA regions came online with their sales teams, increasing the proportion of total revenues from those regions to 26% and 13% of the total revenues in fiscal 2021, respectively, up from 7% and 7%, respectively in fiscal 2020.

Software, subscription and support revenue accounted for 85% of our total revenue in both fiscal 2021 and fiscal 2020. Software, subscription and support revenue accounted for 85% of our total revenue in both fiscal 2021 and fiscal 2020. The cloud-based subscription revenue portion increased by $6.0 million or 154%, in fiscal 2021, from $3.9 million to $9.9 million and accounted for 40% of our total software revenue overall in fiscal 2021, up from 20% in fiscal 2020. The increase in subscription revenue was driven primarily by $4.0 million of revenue from three large contracts from new customers starting in fiscal 2021 and $2.4 million in increased revenue from contracts with existing customers who either upsold or had proceeded into their first full year of revenue recognition. These increases were offset in part by a net revenue decrease of $0.4 million from several smaller customers.

Professional services revenue accounted for 15% of our total revenue in both fiscal 2021 and fiscal 2020. The professional services revenue increased $1.1 million or 32% in fiscal 2021 compared to fiscal 2020, primarily due to a large, $1.5 million consulting contract with a new customer to advise a country in the EMEA region about strategies for protecting their nation. Though several professional services contracts reoccur on a regular basis, most are project specific and last less than a fiscal year.

Cost of revenue

Total cost of revenue increased by $0.4 million or 6%, in fiscal 2021, compared to fiscal 2020. Cost of software, subscription and support revenue decreased by $0.5 million or (8)%, in fiscal 2021, compared to fiscal 2020. The decrease was due primarily to more efficient purchasing of third-party computing costs and increased efficiency in providing software support to customers.

Cost of professional service revenue increased by $0.9 million in fiscal 2021, compared to fiscal 2020. The increase in cost of service revenue was primarily due to an increase in overall professional services activity in fiscal 2021 compared to fiscal 2020 combined with an increasing proportion of traditional services margin contracts in the mix, resulting in a decline in the overall services margin to 64%.

Gross Profit and Gross Margin

Favorable changes in the cost of revenue resulted in an increase in software gross margin to 78.1% in fiscal 2021 compared to 70.2% in fiscal 2020. We expect that gross margins for fiscal 2022 will continue to be above the fiscal 2020 level. However, margins may remain volatile compared to fiscal 2021 due to the continuing presence of large contracts in our revenue mix.

The following tables show gross profit and gross margin, respectively, for software products and support revenue and professional services revenue for fiscal 2021 as compared to fiscal 2020.

	Year Ended January 31,		2021 vs 2020	
	2021	2020		
	(in millions)			
Software products margin	$19.3	$13.9	$ 5.4	39%
Professional services margin	2.9	2.6	0.3	12%
Total Gross profit margin	$22.2	$16.5	$ 5.7	35%

	2021	2020	Change
Software products margin	78.1%	70.2%	7.9%
Professional services margin	64.4%	79.4%	-15.0%
Total Gross profit margin	76.0%	71.6%	4.4%

Operating expenses

Research and development

Research and development expenses decreased by $0.8 million or (3%), in fiscal 2021, compared to fiscal 2020 as we reorganized our engineering departments towards our cloud-based and increasingly SaaS-delivered software offerings and paused net hiring as we completed that transition. At 88% of total revenues in fiscal year 2021 compared to 115% in fiscal 2020, we expect that our overall R&D expenditure rate as a percentage of revenues will continue to decline in the future.

Sales and marketing

Sales and marketing cost increased by $12.5 million or 70% in fiscal 2021, compared to fiscal 2020, primarily due to the continued build out of our sales force globally. We either expanded or initiated activity in

public company reporting and accounting operations experience. We are also implementing the required segregation of roles and duties both in manual and systems related processes including for journal entries and account reconciliation, and formalizing the documentation and performance of remaining information technology general controls for information systems utilized for financial reporting. We believe the measures described above will remediate the material weakness identified and strengthen our internal control over financial reporting. We are committed to continuing to improve our internal control processes and will continue to diligently and vigorously review our financial reporting controls and procedures.

Quantitative and Qualitative Disclosures about Market Risk

We have operations in the United States and internationally, and we are exposed to market risk in the ordinary course of our business.

Foreign Currency Risk

The significant majority of our sales contracts are denominated in U.S. dollars, with a small number of contracts denominated in foreign currencies. A portion of our operating expenses are incurred outside the United States, denominated in foreign currencies and subject to fluctuations due to changes in foreign currency exchange rates, particularly changes in the Singapore Dollar, British Pound, Japanese Yen and Australian Dollar. Additionally, fluctuations in foreign currency exchange rates may cause us to recognize transaction gains and losses in our consolidated statements of operations. The effect of a hypothetical 10% change in foreign currency exchange rates applicable to our business would not have a material impact on our historical consolidated financial statements for year to date 2022 or fiscal year 2021. As the impact of foreign currency exchange rates has not been material to our historical operating results, we have not entered into derivative or hedging transactions, but we may do so in the future if our exposure to foreign currency becomes more significant.

Emerging Growth Company ("EGC") Status

We are an emerging growth company, as defined in the JOBS Act. Under the JOBS Act, emerging growth companies can delay adopting new or revised accounting standards issued subsequent to the enactment of the JOBS Act until those standards apply to private companies. We have elected to use this extended transition period for complying with certain new or revised accounting standards that have different effective dates for public and private companies until the earlier of the date we (i) are no longer an EGC or (ii) affirmatively and irrevocably opt out of the extended transition period provided in the JOBS Act. As a result, our consolidated financial statements may or may not be comparable to companies that comply with new or revised accounting pronouncements as of public companies' effective dates.

BUSINESS

Overview

We are transforming cybersecurity through Collective Defense using our behavioral analytics technology.

We compete in the Network Detection and Response ("**NDR**") category, which is a growing aspect of modern enterprise security, but which does include major competitors. Our value proposition and competitive differentiator is our collective defense concept. The founder of Legacy IronNet and our Co-CEO, Gen. Keith B. Alexander (Ret.), serves as a valuable business development resource for establishing relationships with larger enterprise and government buyers. The significant majority of our current revenue comes from our IronDome and IronDefense products. IronDefense is an NDR cybersecurity product that uses artificial intelligence ("**AI**"), machine learning ("**ML**"), behavioral analytics, and operational tradecraft expertise to quickly identify specific network behaviors or events indicative of malicious threats. Enriched by our cyber tradecraft knowledge, alerts produced by our company help analysts quickly contextualize and prioritize threats that pose the greatest risks. By doing this we are able to provide clients, across a variety of industries, nation-state-level defensive capabilities to reduce cyber risk.

The Cyberspace Solarium Commission suggests the importance of this service in the following statement in its March 2020 report:

"The reality is that we are dangerously insecure in cyber. Your entire life—your paycheck, your health care, your electricity—increasingly relies on networks of digital devices that store, process and analyze data. These networks are vulnerable, if not already compromised. Our country has lost hundreds of billions of dollars to nation-state sponsored intellectual property theft using cyber espionage."

We are a metric-driven organization with a differentiated and potentially transformational approach to the cybersecurity problem facing every organization today. With an ever-increasing cybersecurity threat posed by advanced persistent threat ("**APT**") actors, a team of experts assembled by Gen. Alexander, the longest serving Director of the National Security Agency ("**NSA**") and Commander of Cyber Command in U.S. history, can help solve this problem. It takes knowledge of how APTs operate and their tactics, techniques and procedures in order to defeat them; few individuals and even fewer companies have that knowledge or capability. Our differentiated market offering called IronDome offers users a collective defense model to help mitigate threats posed by an APT enhanced by its IronDefense platform, offering our clients new protections against an APT with its technology.

According to a report commissioned by LGL to 5by5 Cyber Consulting, the question, "Does IronNet have reasonable defensive measures in place across people, processes and technology?" concluded that we have invested a lot of time and effort into our security architecture, have obtained an impressive array of certifications and have undergone extensive audits and testing to ensure we are meeting industry standards. We have highly skilled people in critical security roles and mature processes in place for crucial areas like change management, data protection and software development. We also have a robust technology stack to defend our network and skilled analysts to operate them. We take training seriously and require annual training for all members of the organization on information security and have a defined training track for our security analysts. While this is not a guarantee a company will not have a security breach, 5by5 concluded that we have taken reasonable precautions to protect against it.

Cyber Landscape Overview

"Cybersecurity is one of the most systemically important issues facing the world today. Cyber information sharing is critical to helping better collective security in the digital ecosystem in which society increasingly relies."

—World Economic Forum

From an independent assessment of our platform performed by TAG Cyber, it is clear that cyber security has advanced from a niche technical concern to a mainstream consideration for organizations of all sizes and in all sectors. Security protection concerns are most intense where safety or life-critical consequences might arise in response to a cyber threat. Power companies, financial services firms, telecommunications companies, military organizations, and government agencies thus have the greatest need for security protection, and now make considerable investments in cyber.

The primary security challenge in modern organizations is the complexity that has evolved in the typical business or government entity. Applications, networks, systems, endpoints, and data have experienced considerable sprawl as the costs associated with computing have decreased significantly. This is especially true for cloud-based infrastructure and SaaS-based applications, where cheap ubiquitous services are now available on-demand and for nearly every purpose imaginable.

Modern organizations must therefore develop security protections that address such growth, often delivered in the context of digital transformation initiatives. An additional complication is that hackers have been augmented by determined, capable adversaries, often funded or otherwise backed by criminal groups or nation- states. Serious consideration must thus be given to the types of protections that are necessary to defend against the threat from such capable threat actors.

An additional dimension is that the velocity associated with computing infrastructure and their associated threats has accelerated. Agile DevOps processes generate new features at increasing rates, sometimes hourly for popular services, and hackers use automated platforms to bombard targeted infrastructure with alarming intensity. Security engineers thus require controls that are automated and that address this challenge of increased speed. Manually controlled point solutions no longer stop threats.

A further complication is the massive and increasing scale associated with the types of systems operated by larger enterprise teams. Large-scale IT and network systems remove the ability for organizations to rely on manual maintenance, fixed configurations, and simple asset management. Furthermore, the visibility of assets that might be well-known by smaller organizations can only be approximated in large scale settings. This greatly complicates the challenge of delivering security in a large-scale setting.

In response to these challenges, modern Chief Information Security Officers ("**CISOs**") put considerable time and effort into designing and implementing a workable security architecture. Individual CISO-led teams—even if they focus their efforts – have come to recognize that they cannot address the cyber challenge on their own. It is well-understood in the cybersecurity community that enterprise security teams need considerable external assistance, coordination and cooperative guidance.

Some of this assistance is obvious: Businesses rarely develop their own security tools, but rather buy from vendors or adjust open-source tools. Similarly, information sharing groups have emerged to support cooperative discussions between experts. It is therefore not controversial to suggest that business and agencies need to work together to address cyber threats. The big question, instead, is how this objective can be best achieved. This is one of the challenges addressed by IronNet.

Background of IronNet

We are a global cybersecurity company revolutionizing how organizations secure their networks by delivering the first-ever Collective Defense platform operating at scale. Employing a number of former National Security Agency ("**NSA**") cybersecurity operators with offensive and defensive cyber experience, we integrate deep tradecraft knowledge into its industry-leading products to solve the most challenging cyber problems facing the world today.

Gen. Alexander founded Legacy IronNet in 2014 to solve the major cybersecurity problem he witnessed and defined during his tenure as former head of the NSA and founding Commander of U.S. Cyber Command: You can't defend against threats you can't see. Our innovative approach provides the ability for groups of organizations—within an industry sector, supply chain, state or country, for example—to see, detect and defend against sophisticated cyber attacks earlier and faster than ever before.

We have defined a new market category called Collective Defense. As the first mover in this category, we have developed our Collective Defense platform, the first, and to our knowledge, the only solution that can identify anomalous (potentially suspicious or malicious) behaviors on computer networks and share this intelligence anonymously and in real time among Collective Defense community members. Collective Defense communities comprise groups of organizations that have common risks, such as a supply chain, a business ecosystem, or across an industry sector, a state, or a country. This cybersecurity model delivers timely, actionable, and contextual alerts and threat intelligence on attacks targeting enterprise networks, and functions as an early-warning detection system for all community members.

This new platform addresses a large and unwavering compound problem: limited threat visibility for increasingly borderless enterprises across sectors and at the national level, paired with ineffective threat knowledge sharing across companies and sectors and a "go it alone" approach to cybersecurity. These operational gaps, combined with market dynamics like the increased velocity of sophisticated cyber attacks and the deepening scarcity of qualified human capital, have set our mission to transform how cybersecurity is waged.

Understanding Collective Cyber Defense

Ideally the U.S. Government could defend the nation against cyberattacks similar to what was developed for the Intercontinental Ballistic Missile ("**ICBM**") missile threat. Unfortunately, the ability to enact such a defense would likely require limiting personal freedoms on the internet that Americans currently enjoy. Legislation limiting personal freedoms would likely be challenging to pass and thus the probability of that happening in the near future is low. The Cyberspace Solarium Commission report submitted in July 2020 contains over 80 recommendations to address the issue of cybersecurity, with one of them being "Reshaping the Cyber Ecosystem." That report states:

"Raising the baseline level of security across the cyber ecosystem—the people, processes, data, and technology that constitute and depend on cyberspace—will constrain and limit adversaries' activities. Over time this will reduce the frequency, scope, and scale of their cyber operations. Because the vast majority of this ecosystem is owned and operated by the private sector, scaling up security means partnering with the private sector and adjusting incentives to produce positive outcomes."

Our collective defense model, IronDome, is a means for the private sector to "raise the baseline" level of security by partnering amongst themselves to "produce positive outcome." This overwatch function is a differentiator for our portfolio of offerings, making us one of the few companies that has the ways, ends and means to enact this transformational concept due to the technical capabilities required to ensure its success.

To properly understand our platform and solution approach, it is best to begin with an outline of how collective defense can reduce cyber risk for larger organizations. This approach benefits from many years of organizations beginning to share data through various groups such as Information Sharing and Analysis Organizations ("**ISAO**"). We are the first major commercial vendor to offer an end-to-end means to take full advantage of the collective concept.

Toward a Collective Cyber Defense

Businesses and agencies will only cooperate on collective cybersecurity initiatives if they see meaningful benefits with low associated risk. Admittedly, this is how almost all business decisions are made, but large-scale

cybersecurity introduces an added benefit for collective defense—namely, that cyber protection schemes work much better when they involve a wider range of intelligence, visibility, and security coverage. Working together in cybersecurity thus introduces clear benefits for participants.

Nevertheless, cooperation between businesses, agencies, and other groups must address two ends of the spectrum: upside benefits and downside risks for each of the entities and groups involved. In both instances, the case can be made that, for large-scale infrastructure, both benefits and risks can cascade, perhaps even accelerating as lateral traversal of an attack occurs. That is, threats to someone else's system, however remote, might cascade across networks and systems.

Within a large organization, collective protection across business units can have comparable benefit, particularly in companies that evolved through mergers and acquisitions, where a collective defense can help to bring together disparate data sources, defensive perspectives, and protection platforms into a common defense. Such intra-enablement within a large organization is a major focus area for IronNet.

The primary benefits of a collective defense for large-scale cyber defense, whether stretched across a sector, combined between multiple organizations, or combined across the business units of one company, include the following:

Early Warning System—An organization can develop a more effective early warning system if other groups share their indicators in real-time. Not engaging in such sharing limits the ability of a local team to capitalize on early warning that a cascading attack might be underway.

Broader Visibility—By working together with other groups, the local security team benefits from broader visibility, including an improved understanding of how local enterprise changes (e.g., DNS- related) might cascade to other targets.

Strength in Numbers—The fact that cooperation increases visibility into a cyber threat means that organizations who cooperate with external groups are able to leverage strength-in-numbers and thereby provide better security support.

The corresponding risks that must be managed in the development of any large-scale cooperative arrangement for cybersecurity include the following:

Privacy of Shared Data—The possibility emerges that sharing information with a cooperative might result in leaked data or a serious privacy incident. For highly regulated industries, sharing with government may also expose businesses to some regulatory risk (although this is partially mitigated by certain provisions of the Cybersecurity Information Security Act of 2014 ("**CISA**")) if the data is not properly anonymized or otherwise does not comply with legal requirements. Controls must be in place to ensure that cooperating teams are not exposed to this risk.

Attribution of Incidents—Public attribution of an embarrassing or problematic cybersecurity incident to a sharing entity may reduce (or even remove) the willingness of that organization (and others) to share further information about something that might reflect poorly on their own actions. This is less an issue for collective defenses implemented across the business units of one organization.

Competitive Relationship—The risk of one company directly assisting its competitor through participation in a collective defense scheme (e.g., AT&T assisting Verizon, or General Motors assisting Toyota) cannot be ignored. The legal and marketing teams from participating organizations would be wise to adopt the airline and energy industry's observations that a mutual focus on safety helps every participant.

The benefits and risks of cooperation for large-scale cybersecurity across heterogenous groups must be carefully balanced in setting up a collective defense. Too often, collectives are developed that leave participants wondering

what's in it for them, and how potential problems might be avoided. One main value proposition from IronNet is that cooperative cybersecurity will work best when such concerns are carefully curated by a trusted provider with a world-class platform.

Role of Government in Collective Defense

One challenge federal governments have in supporting collective cyber defense is that most large businesses are multi-national. This suggests that while national allegiance might be easily identified (e.g., Verizon is American, Huawei is Chinese), such allegiance must address the interests of the company's shareholders. This emphasis is often misunderstood by government agencies who are focused exclusively on national interests.

Federal governments also have the additional role to regulate and sometimes punish organizations not meeting their security requirements. This obligation complicates government cooperation with business on cybersecurity, at least to the extent that governments are permitted to regulate based on voluntarily shared information. Organizations would thus be hesitant to share information with a cooperative involving government if the reported incident might lead to regulatory investigation.

The biggest challenge, however, is that the majority of critical infrastructure is owned and operated by the private sector. This implies that security telemetry, indicators, and early warnings will come from the private sector, even for many military applications and defensive government activities. This fact is often not understood by citizens and politicians who may demand that government step in and fix large-scale cybersecurity threats. This is usually just not practically feasible.

Government must work hard to share the information it uniquely controls, such as classified indicators that might be downgraded for sharing externally or be shared in a more limited context to defend critical infrastructure. Businesses must also recognize that their obligations extend beyond just the shareholder. This recognition that cooperative sharing is in the best interests of the organization and society in general is an important driver behind our platform offering.

Overview of our Platform Offering

The Collective Defense platform comprises two flagship products:

IronDefense is an advanced NDR solution that uses AI-driven behavioral analytics to detect and prioritize anomalous activity inside individual enterprises. We leverage advanced Artificial Intelligence/Machine-Learning ("**AI/ML**") algorithms to detect previously unknown threats that have not been identified and "fingerprinted" by industry researchers), in addition to screening any known threats, and applies its Expert System to prioritize the severity of the behaviors—all at machine speed and cloud scale.

IronDome is a threat-sharing solution that facilitates a crowdsource-like environment in which the IronDefense threat detections from an individual company are shared among members of a Collective Defense community, consisting of our customers who have elected to permit their information to be anonymously shared and cross-correlated by our IronDome systems. IronDome analyzes threat detections across the community to identify broad attack patterns and provides anonymized intelligence back to all community members in real time, giving all members early insight into potential incoming attacks. Automated sharing across the Collective Defense community enables faster detection of attacks at earlier stages.

Our Collective Defense platform is designed to deliver strong network effects. Every customer contributing its threat data (anonymously) into the community is able to reap benefits from the shared intelligence of the other organizations. The collaborative aspect of Collective Defense, and the resulting prioritization of alerts based on their potential severity, helps address the known problem of "alert fatigue" that plagues overwhelmed security analysts.

The Collective Defense platform is available for on-premise, cloud (public or private), and hybrid environments, and is scalable to include small-to-medium businesses and public-sector agencies as well as multinational corporations. We provide professional cybersecurity services such as incident response and threat hunting, as well as programs to help customers assess cybersecurity governance, maturity, and readiness. Our CS services are designed to create shared long-term success measures with its customers, differentiating it from other cybersecurity vendors by working alongside customers as partners and offering consultative and service capabilities beyond implementation.

The Collective Defense platform is available via a subscription-based pricing and flexible delivery model, with options available for major public cloud providers such as Amazon Web Services and Microsoft Azure; private cloud, or Hyper Converged Infrastructure ("**HCI**") such as Nutanix; and on-premise environments through hardware and virtual options. To make it as easy as possible for customers to add Collective Defense into their existing security stack, IronNet built a rich set of Application Programming Interfaces ("**APIs**") that enable integrations with standard security products, including security information and event management ("**SIEM**"); security orchestration, automation, and response ("**SOAR**"); endpoint detection and response ("**EDR**"); next- generation firewall ("**NGFW**") tools; and cloud-native logs from the major public cloud providers.

We describe out go-to-market strategy as "land and expand with network effects." Our approach is to initially secure influential "cornerstone" customers and then expand into their respective Collective Defense communities with additional "community members" from organizations of similar industry sector, state, country, supply chain, or tailored business ecosystem. As each Collective Defense community grows, so does the volume of shared data, and the value of our platform for each of those members thereby expands both technically and commercially.

We sell into both public and private organizations and the business ecosystems that support them. We have identified tens of thousands of prospective cornerstone customers and more than 100,000 potential community customers.

Some of the world's largest enterprises, government organizations, high-profile brands, and governments trust us to protect their networks. Our customers include a top global hedge fund, eight of the top 10 U.S. energy companies (based on revenue), a leading Asian mobile phone carrier, two U.S. Department of Defense ("**DoD**") branches, a mid-sized bank in the EMEA region, four U.S. state agencies, U.K. and Singapore government entities, and a large global holding company.

We began targeting large enterprises and Fortune 500 companies, but the flexibility and scalability of our cloud-native platform and enhanced go-to-market approach enabled us to expand its customer base to smaller companies as well. We have been recognized in the cybersecurity industry by independent third-party analysts, including Gartner, Forrester, IDC, 451 Research Group, and Omdia, who has called our analytics a "potential game changer" in a June 2020 report. In January 2021, the global insurance brokerage Marsh named the Collective Defense platform as one of its industry-recognized Cyber Catalyst solutions. In August 2020, we announced that we had achieved "FedRAMP-ready" for Agency Authorization status, as approved by the Federal Risk and Authorization Management Program ("**FedRAMP**").

Industry Background

Cybersecurity trends

There are a number of key trends driving the need for a new approach to cybersecurity.

Increased velocity of sophisticated attacks

Increasingly, adversaries are well-trained, possess significant technological and human resources, and are highly deliberate and targeted in their attacks. Adversaries today range from militaries and intelligence services of well-

funded nation-states, to sophisticated criminal organizations motivated by financial gains, to hackers leveraging readily available advanced techniques. The broad availability and rapid evolution of cyber attack toolkits and use of regional cloud infrastructure or compromised servers to launch attacks make it nearly impossible for security teams to keep up with cyber threats. Given sufficient amount of time and resources, a determined adversary will have the ability to breach current cyber defenses of almost any enterprise, organization, or government.

Rear-facing and insufficient tools

Gartner, an industry research firm, estimates that worldwide spending on global information security will be $186.2 billion by 2024, up from $124.2 billion in 2018. Even with increased cybersecurity spending, however, security outcomes have not substantially improved. The recent widespread SolarWinds/SUNBURST cyberattack is just one example of how a sophisticated adversary can thoroughly permeate an industry, geography or supply chain. The lack of equally sophisticated threat intelligence sharing allowed this hack to penetrate networks more deeply, and for much longer. The evolving threat landscape has rendered traditional defense approaches incapable of protecting organizations against next-generation threats.

The current generation of security products focuses on signature-based approaches that often have limited ability to collect, process, and analyze vast amounts of data—attributes that are required to be effective in today's increasingly dynamic threat landscape. This includes traditional and next-generation firewalls, Intrusion Detection and Prevention Systems ("**IDPS**"), SIEMs, and other similar tools that are designed to manage policies for network traffic and rely on rear-facing threat intelligence indicators of compromise ("**IoCs**") based on IP, domains, file hashes and other signature-based intelligence from known threats. They are not fundamentally designed to detect advanced, never-before-seen, "unknown unknown" cyber threats in a timely and scalable fashion.

The borderless enterprise where the network is no longer the perimeter

Cloud, IoT and SaaS applications have expanded the attack surface and cyber vulnerabilities. According to a Gartner press release dated May 13, 2020, Gartner reports that, while some cloud transformation projects may have put on hold during the COVID-19 pandemic, it expects overall cloud spending levels previously estimated for 2023 and 2024 to show up as early as 2022. The ongoing COVID-19 pandemic has only accelerated this trend, with one survey by PricewaterhouseCoopers LLP reporting that 83% of executives believed the shift to remote work had been successful and that 79% of executives would no longer require a traditional five-day onsite work week. Furthermore, IDC, an industry research firm, estimates that by 2025 there will be 55.7 billion connected devices worldwide. The reality of the borderless enterprise will fundamentally change network cyber defenses from a centralized command and control defensive strategy using traditional on-premise blocking infrastructure to a distributed detect and respond strategy that fuses different sources of telemetry data across network, endpoints, and logs into actionable intelligence using large-scale behavioral analysis for security teams to take action.

Scarcity of qualified human capital

Even with the most sophisticated AI-based cyber technology in place, the human element of cybersecurity investigation, triage, and research plays an important role in risk reduction. As the Collective Defense platform is detecting and prioritizing anomalies, the analysts and threat hunters are ultimately deciding which alerts to triage, investigate, and manage through to response and mitigation. Organizations are consistently under-resourced in this area, however, as the ratio of the volume of network traffic versus the number of cybersecurity specialists to analyze that traffic is severely lopsided, resulting in Security Operations Center ("**SOC**") staff overwhelm and burnout. A July 2020 report by the Information Systems Security Association states that 70 percent of its members believe that their organization has been impacted by the global cybersecurity skills shortage. The number of unfilled cybersecurity positions has already surpassed four million worldwide.

Cloud impact on enterprise cyber defenses

As digital transformation has accelerated in all industries, traditional security controls implemented on the company's on-premise network are often no longer available and often must operate differently for the outsourcing of IT infrastructure and operations to the public cloud provider. While the cloud is designed to make business easier, Management and Security Operations are different from traditional on-premise security, as the teams do not have access to the underlying networks or logs, and therefore have limited visibility of cloud infrastructure. The major cloud providers have introduced logging and basic detection using signature-based detection strategies, but these require additional third-party or custom capabilities to provide sufficient defenses. Security vendors have attempted to fill the security gaps by introducing new products for the cloud based on existing on-premise technologies, but these are often cloud bolt-ons that provide limited detection and visibility for cloud environments and are complex to deploy, difficult to scale, brittle to maintain, and costly to own.

Limitations of existing products

Existing detection and threat sharing methods have a number of limitations, including:

Legacy signature-based products

Signature-based products are designed to detect known attacks using a repository of previously identified indicators of compromise, but are not capable of detecting or responding to unknown threats. Used by network security, endpoint security, SIEMs and other standard defense-in-depth cybersecurity solutions as a core detection method, these signature-based detections have resulted in many significant breaches due to the failure of legacy defenses to detect a previously unknown or modified version of a previously known attack. While current technologies remain an essential part of the SOC Visibility Triad, a network-centric approach to threat detection and response described by Gartner in 2019, they miss a large swath of dangerous threats that evade detection, as evidenced by the major SolarWinds/SUNBURST supply chain and Microsoft Exchange server attacks widely reported in the news media in 2020 and 2021.

Log and event management products

SIEMs and similar log management products are designed for compliance, reporting, and security incident management purposes, but they struggle with the scale and processing required to deliver the behavioral-analysis capabilities across current and historical data to detect new or modified versions of known threats. While these systems provide useful correlation capabilities, security operation teams are increasingly leveraging these systems for central aggregation points for workflow, ticketing, and case management, rather than for detection.

First generation network-based behavioral analysis products

First generation network-based behavioral analysis products provide a basic level of outlier detection using Bayesian analysis or other statistical methods to identify obvious patterns in small networks. Often marketed as artificial intelligence ("**AI***")* solutions, these solutions lack the scale, correlation, or analysis capabilities needed to detect threats hiding in plain sight within networks commonly seen at mid-sized or larger enterprises with thousands of devices, hundreds of applications, multiple physical sites, and multi-cloud architectures.

Infrastructure monitoring/network performance monitoring and diagnostic-based products

Traditional network infrastructure providers offer infrastructure monitoring products designed to identify network bottlenecks and other network reliability or performance issues. Increasingly, these vendors have added bolt-on cybersecurity capabilities that can provide security teams' networks with asset discovery and some network visibility, but they struggle with the algorithmic analysis needed to detect new and unknown threats with high fidelity or the forensic capabilities required by security operations team to investigate, triage, and respond to an identified network anomaly.

Threat intelligence sharing products

Threat intelligence products are designed to share massive amounts of non-specific signature-based IoCs that commonly focus on IP addresses and domains of known threats and often only after a substantial period of time by the contributing organization. The lack of timeliness or specificity to an enterprise severely limits the effectiveness of the shared information from a cyber defense perspective. By the time this information is shared, usually weeks or months after an attack, a sophisticated attacker only needs to slightly modify their methods by changing their attack infrastructure to enable them to bypass cyber defenses of their targeted enterprises, industries, or nations.

Information Sharing and Analysis Centers ("ISACs") and other threat sharing groups

Threat sharing groups emerged more than 20 years ago as a way for security teams to work together to collect, analyze, and share actionable threat information within their members communities. We believe this is a substantial step in the right direction; however, threat sharing in these groups relies largely on signature-centric threat intelligence platforms that struggle with timeliness and specificity of their intelligence or ad hoc manual forms of communication, such as email and only with a subset of security defenders with whom an analyst has a personal relationship. ISACs and similar groups are the right organizations, but they need technological solutions that enable them to share contextual, relevant, and timely information in real time across the full community.

Creating a new market segment: Collective Defense

"The U.S. government and industry must arrive at a new social contract of shared responsibility to secure the nation in cyberspace. This 'collective defense' in cyberspace requires that the public and private sectors work from a place of truly shared situational awareness and that each leverages its unique comparative advantages for the common defense."

—U.S. Cyberspace Solarium Commission Report, March 2020

We are creating a new market category with Collective Defense. With its Collective Defense platform, we developed the first and, to its knowledge, the only solution that can identify and rate anomalous behaviors on the network and share this anonymized threat intelligence among Collective Defense community members (who may comprise a supply chain, state, or country) as an early-warning system for all.

The power of Collective Defense is that multiple companies can essentially work as a team to detect and defend against attackers early in the network threat intrusion cycle. This differentiated approach allows customers to:

Gain real-time visibility across the threat landscape

Our Collective Defense platform leverages proven behavioral analytics, machine learning ("**ML**"), and AI techniques across anonymized participant data to identify stealthy, sophisticated threats that otherwise may be missed by an individual enterprise and signature-based tools. The platform has been designed to deliver real-time visibility of cyber threats targeting supply chains, industries, regions, or any custom IronDome Collective Defense grouping.

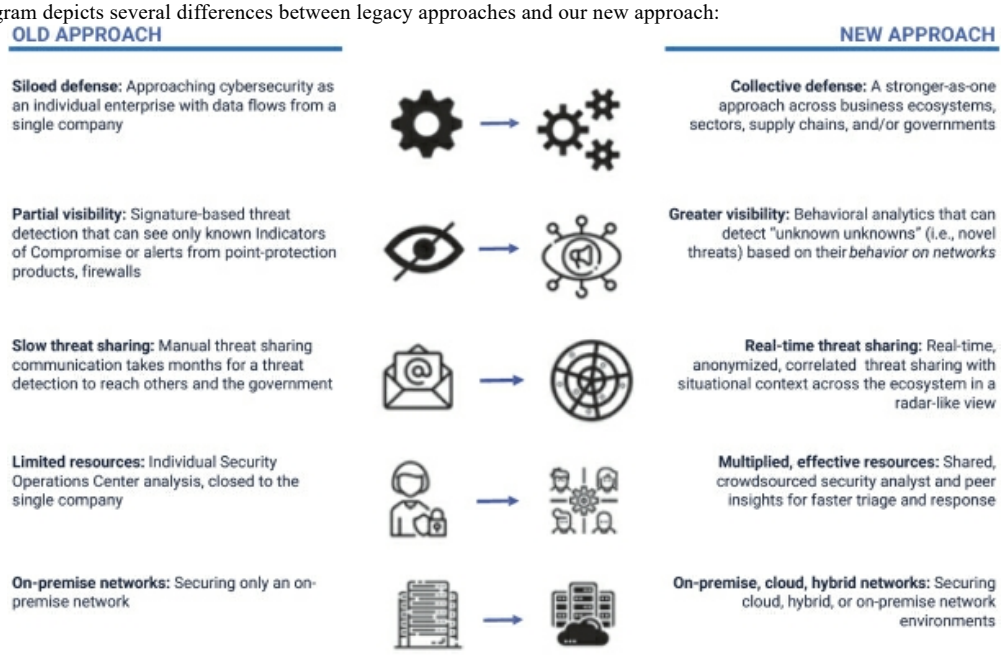
Reduce impact of cyber attacks with help from fellow cyber defenders

The Collective Defense ecosystem acts as a collaboration hub to enable participants to automatically share real-time detections, triage outcomes, threat indicators, and other insights with members of their Collective Defense group. When suspicious behaviors are identified by any member, IronDome automatically shares a proactive warning to all members at machine speed so each member can prioritize their defense against the identified cyber threat.

Improve effectiveness of existing cybersecurity investments

Threat intelligence is valuable, actionable, and relevant only when received in time, before a threat enters a network. Our innovative collective threat intelligence provides immediate alerts at machine speed and context into urgent threats, enabling organizations to prioritize threats and build a proactive defense. This information can be used by a customer's existing network, endpoint, or other security tools to identify and stop adversaries from retargeting their attack.

The following diagram depicts several differences between legacy approaches and our new approach:



A new cybersecurity model: from reactive, individual defense to proactive, Collective Defense

Our Solution: The Collective Defense Platform

The Collective Defense platform comprises two tightly integrated proprietary technologies: Our NDR solution, IronDefense, and our innovative collective threat-sharing solution, IronDome.

Our Collective Defense platform offers a unified set of technologies that powers a wide range of network behavioral detection, security operations, real-time threat landscape visibility, threat sharing, and peer SOC-analyst collaboration capabilities. We can rapidly and cost effectively deploy in our customer's public cloud, private cloud, and on-premise infrastructure using our flexible deployment options. Our expanding set of open APIs and ecosystem integrations enable us to add new sources of data for behavioral analysis and Collective Defense sharing and collaboration to detect and stop targeted cyber attacks.

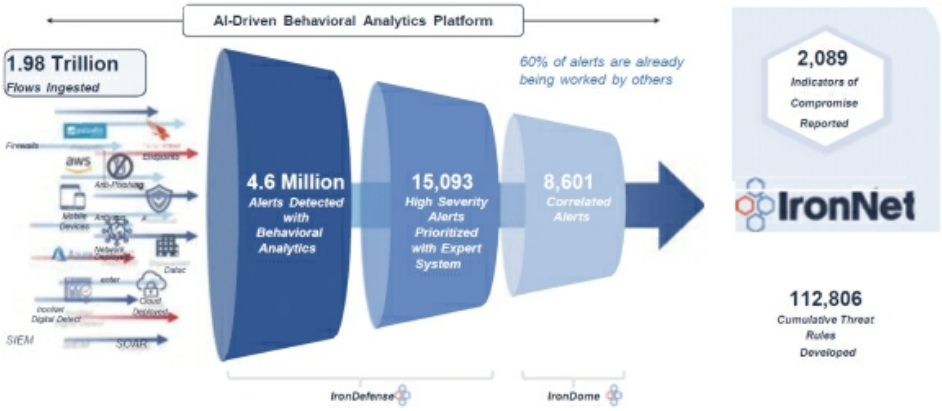
Armed with elite detection capabilities and combined offensive operator experience at the highest level of the U.S. government, our founders set out to build a behavioral analytics solution to detect threats heading toward, or already in, the network. A growing portfolio of proprietary analytics forms the backbone of IronDefense.

However, while effective in detecting unknown anomalies, behavioral analytics by itself is insufficient in modern, noisy networks where anomalies are common and can lead to a high number of false positives. For many NDR vendors in the industry, the solution is to tune their analytics to be less sensitive in order to deliver reduced false-positive rates at the expense of letting true positives into the network. We undertook a different strategy to meet this challenge. We introduced our expert system scoring algorithms, supported by our elite cyber hunters, to increase its detection specificity while preserving the sensitivity of its analytics in IronDefense.

We introduced IronDome in 2018. Powered by IronDefense's threat detections, IronDome is the foundation of our Collective Defense platform, a purpose-built, cloud-native, and holistic platform that is capable of defending, analyzing, and correlating threats from various sources. It delivers timely, actionable, and contextual insights to attacks targeting an enterprise and, from there, is able to provide early warning to all members of the Collective Defense ecosystem.

The differentiated value of our Collective Defense platform is its ability to build a dynamic, comprehensive picture of the threat environment, much like radar for cyberspace, based on real-time, anonymized alert correlation across any participating member environments. It also provides situational context and peer insights for greater visibility and context of the threat landscape at any given time.

The following diagram depicts threat detections on our Collective Defense platform during 2020:



Notes:Represents full-year data for calendar year 2020 except for cumulative number.

Correlated alerts for threat detection earlier in the intrusion cycle

We are not aware of any other vendor in the market with a similar approach to cybersecurity. Even though community members bring disparate network environments, such as cloud, on-premise or hybrid, to the Collective Defense ecosystem, correlated threats stand out given that the adversarial behaviors are typically consistent, no matter who the target is, as was the case with the SolarWinds/SUNBURST attack.

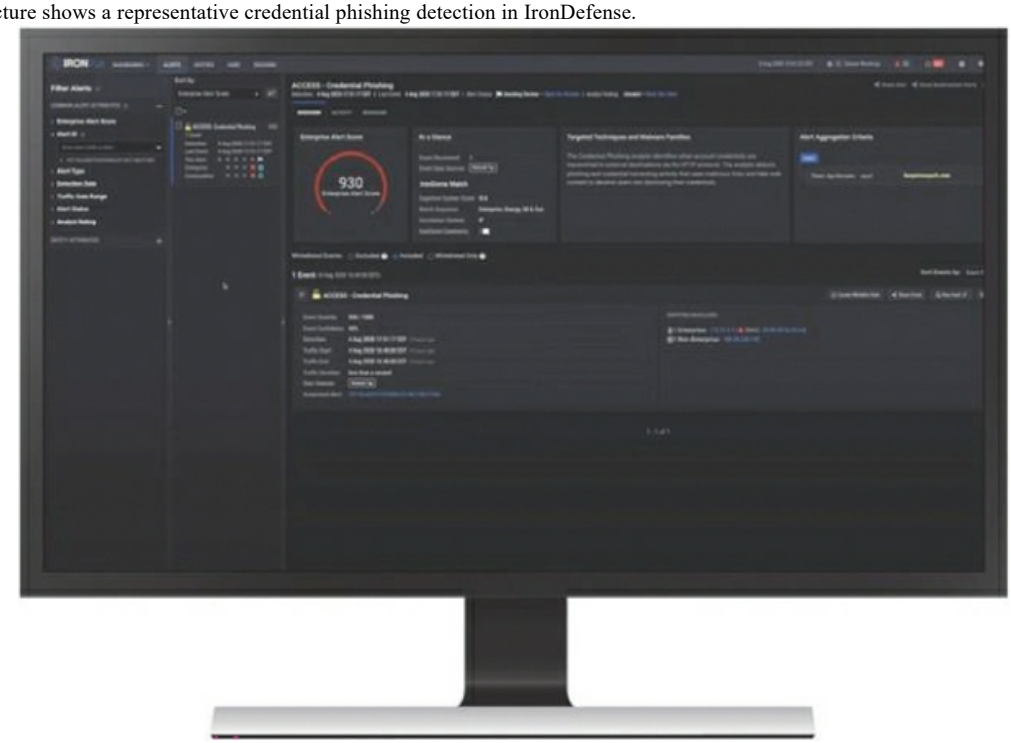
The Collective Defense platform comprises two flagship products:

IronDefense

IronDefense is an advanced NDR solution that provides behavior-based and AI-driven analytics at the network level to detect anomalous activity at individual enterprises and prioritize the highest threats in a company's

network. We leverage a novel AI/ML algorithms to deliver high-fidelity analytics required to detect previously unknown threats. In addition, we provide advanced enrichment techniques via IronDefense's Expert System, which has been designed to achieve high efficacy levels, low false positive rates, and improved visibility compared to legacy approaches. This is all done at network speed and cloud scale.

The following picture shows a representative credential phishing detection in IronDefense.



Most current cybersecurity tools focus on detecting the final "action-on-target" step of an intrusion. At this stage, identification is easier but the insights come far too late to stop attackers from getting into positions in the network to exfiltrate data, steal IP, or accomplish other malicious objectives. IronDefense uses advanced analytics based on metadata from the traffic in the customer's network to identify anomalous activity earlier in the intrusion kill chain.

Key components of IronDefense include:

IronDefense behavioral analysis engine

IronDefense leverages behavioral-based detections to identify threats targeting industries and companies earlier in the intrusion cycle, and to identify the underlying behavior and methods to counter unknown threats, or customizations that attackers will implement to target companies in the future. The analytics are built upon algorithms that form the foundation of the patented IronDefense platform. They are computationally designed to understand normal network behavior by applying tests to create a benchmark of standard, acceptable traffic patterns in the network. Detected anomalies are grouped with similar instances of traffic behavior to minimize alerting and to aggregate events by events within the customers' networks.

IronDefense Expert System

IronDefense includes an Expert System that automates security operations playbooks of how top cyber operations hunters leverage contextual data and other sources of telemetry data later on in the detection and response process and applies it to the risk scoring of anomalies detected by its behavioral analysis. This enables us to preservice its detection accuracy without sacrificing the sensitivity of its algorithms by leveraging the wisdom of our elite cyber hunters triaging thousands of alerts from real-world environments. The expert system also alleviates the "alert fatigue" that plagues every SOC by minimizing the tedious steps in an investigation, reducing alert fatigue and allowing security teams to focus on responding to high risk detection in their environments. The Expert System is continually optimized through machine learning from anonymized triaged outcomes by our cyber hunters using IronDefense.

IronDefense CoDA engine

Threat analysts and hunters spend a significant portion of their time triaging individual alerts by identifying corroborating evidence and related information. In 2021, we are launching a new correlation engine called CoDA, for Correlation of Detections and Alerts, that models adversary attack techniques and pre-correlates anomalous activity by threat categories to improve risk scoring and alert prioritization, as well as to dramatically reduce alert load. This system leverages a multi-pass system that first optimizes for detecting as many potential instances of a particular type of threat activity and enriching detections with threat intelligence and other external and internal data sources to optimize for detection precision. Events are further aggregated by entity information, attack stage identification, and time sequence data to deliver a timeline of an attack and scored by risk to the enterprise.

IronDefense threat hunting interface

IronDefense includes a threat hunting interface built by our elite cyber hunters to empower security operations teams to conduct detailed investigative workflows and forensic analysis of threats detected by IronDefense. The hunting interface empowers security analysts to investigate across all raw traffic, network metadata, logs, telemetry data, and collective threat intelligence captured by IronDefense, all the way down to full-packet capture of individual network flows.

IronDefense sensors

IronDefense sensors are cloud, virtual, and physical sensors that are deployed at the network perimeter to ingest "north-south" traffic within internal networks to provide "east-west" traffic visibility across an enterprise. Cloud sensors are available for public cloud environments to ingest raw traffic data directly from Infrastructure-as-a-Service ("IaaS") virtual networks from major cloud providers such as AWS and Microsoft Azure deployments. The sensor extracts rich network session metadata from the raw traffic and sends it to our behavior analysis engine for processing and expert system validation. The IronDefense sensors also continuously collect full raw traffic packet capture for inspection during hunting operations.

IronDefense direct data ingest

IronDefense has the ability to utilize a wide-range of data types and telemetry data directly from existing sources. These data sources include standard protocols such as DNS, HTTP/S, or Active Directory; common network log formats such as BRO/ZEEK or NetFlow; Cloud Provider logs such as AWS VPC, AWS CloudTrail or Microsoft Azure NSG logs; and application logs such as Office 365.

IronDome

IronDome is a threat-sharing solution that facilitates a crowdsourced-like environment in which the IronDefense findings from an individual company are automatically and anonymously shared within groups of related entities,

such as portfolio companies, supply chains, industries, or nations, for correlation and further analysis. IronDome analyzes threat detections across companies to identify broad attack patterns and provides anonymized intelligence back to all customers in real time.

IronDome enables Collective Defense member enterprises to actively share individual anonymized cyber anomalies at machine speed across a community of public-private peers. This capability allows companies to identify stealthy attackers earlier in the attack cycle when many of their methods fall below the threshold of detection at a single company by allowing companies to aggregate data and run higher-order analysis across industry data.

Key components of IronDome include:

IronDome Collective Defense communities

IronDome threat sharing is organized by communities of enterprises based on their business ecosystem, industry, region, or nation. Enterprises can be members of multiple communities based on their sharing preference and threat sharing needs. As customer adoption grows, the network effect of each additional enterprise participating in IronNet's Collective Defense platform will amplify the breadth and depth of its dataset and intelligence.

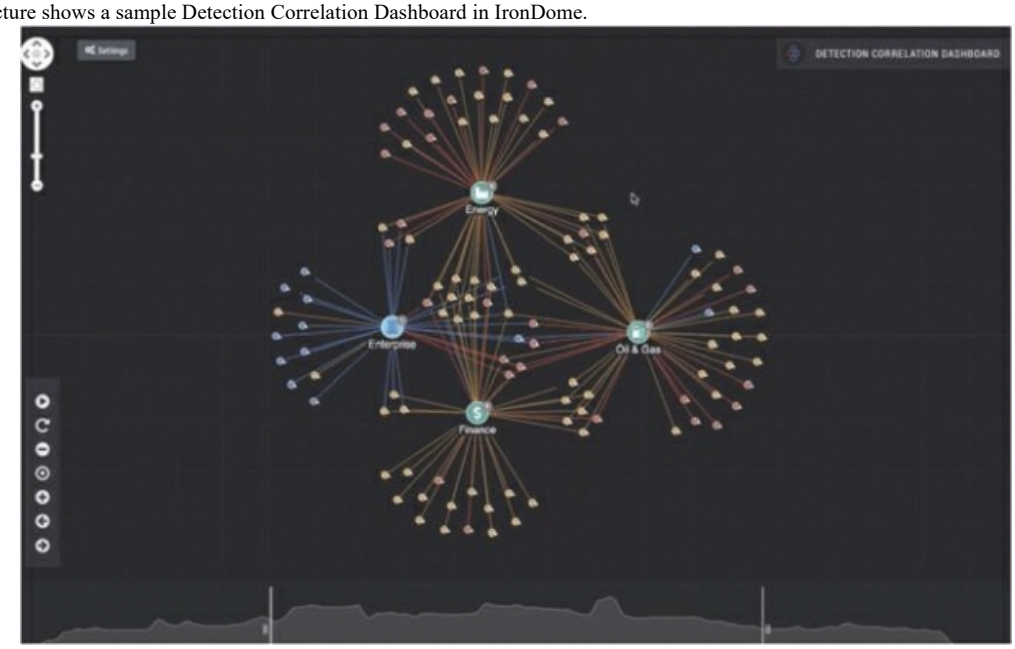
IronDome collective threat intelligence sharing

IronDome links communities of enterprises together to provide contextual insights into the threat landscape. Machine and human intelligence is shared in real time across the community by threat correlations, as well as outcomes and insights related to how various analysts at different enterprises rated and triaged similar threats in their environment. Real-time feedback of these insights delivers enhanced threat landscape visibility and detection insights that allow members to immediately react to active threats targeting their industry and to adjust their defenses to combat the threat.

IronDome RadarView

IronDome creates a radar-like view of cyberspace that links private and public sector stakeholders in their Collective Defense community. The RadarView graph provides an anonymized real-time view of threats targeting an enterprise's business ecosystem, supply chain, industry, or region.

The following picture shows a sample Detection Correlation Dashboard in IronDome.



Called Collective Defense communities, spearheaded by a "cornerstone" company or organization, an IronDome could be established for a company's business ecosystem, such as a wealth management firm with many portfolio companies; a sector-based collaborative, such as in within energy or finance), or a cross-sector formation; states and countries; and private-public sector configurations.

In each Collective Defense community, members agree to share anonymized data about threats detected on their individual networks with the collective, on an ongoing basis. This collaborative approach is designed to "flip the script" on attackers by raising the defensive capabilities of any one player. If correlated alerts and attribution based on behaviors suggest that a nation-state is involved, Collective Defense participants can voluntarily share threat information with the government for cyber defense on a national scale as needed to defend the nation.

The Collective Defense platform is available for on-premise, cloud (public and private), and hybrid environments, and it is scalable to include small-medium businesses as well as multinational corporations.

Threat Intelligence

Using information derived from the Collective Defense Platform, we also provide our customers with threat intelligence.

IronNet Threat Intelligence Rules

We develop threat intelligence rules ("**TIRs**") based on significant community findings. These detection rules for network, endpoint, or other security tools allow customers to proactively protect themselves against known threats through more secure controls.

Expand into new customer segments

While we first targeted large and sophisticated enterprise customers, we also have an internal sales development team and an inside sales team to expand our go-to-market efforts. These teams focus on early qualification and development for cycles with potential cornerstone customers. They utilize intelligence from our Account Based Marketing system as well as social sales development tools to nurture these opportunities to a handoff point with field sales. These teams also focus on full cycles with potential community members once a cornerstone-driven Collective Defense community has been established. We are using a combination selling approach to scale our sales into additional industry verticals, with which we can sell our Collective Defense capabilities to the largest enterprises or smallest businesses with any level of security sophistication and budget.

Extend our Collective Defense platform and ecosystem

We have designed our architecture to be open, interoperable, and highly extensible. It is constantly adding integrations to our platform in order to ingest more sources of data for analysis and to provide detection outputs to more response systems. We also add new algorithms and new combinations of algorithms to detect behaviors of unknown but potentially malicious attacks. In addition, we innovate with partners to add our NDR and Collective Defense capabilities to their customer offerings. An example of this is our recent announcement of a strategic partnership with Mandiant, a part of FireEye, Inc., under which the parties will work together to provide best-in-breed managed cyber defense capabilities to companies and government agencies of all sizes. The new jointly managed collective defense service offering is designed to remove the burden of identifying new and novel threats from public and private security teams by providing a potent software and services combination. We expect that innovations and partnerships such as our partnership with Mandiant will enhance the distribution of our platform and represent future sources of revenue.

Broaden reach into the U.S. federal government vertical

We spent the first five years of our life building foundational customer relationships in the commercial sector. This was intentional, as the company mission required it first to build the technology and business basis required to protect the private side of the public/private partnership. We are now actively investing in the acquisition of customers in the U.S. federal government vertical. We are FedRAMP Ready and are registered with the Department of Homeland Security Continuous Diagnostics & Monitoring program approved products list to provide federal agencies with innovative security tools. In addition, our platform is deployed in the AWS GovCloud. We are pursuing opportunities in the civilian, defense, and intelligence sectors.

Expand our international footprint

We are expanding our international operations and will continue to invest globally to broaden our international footprint. We intend to grow our presence in the Asia Pacific Japan and EMEA regions by adding headcount and establishing overseas hosting relationships.

Our Technology

Cloud-native architecture

Our platform is designed to be secure, highly scalable, redundant, resilient, and high-performing. Delivering from the cloud is intended to enable agility, ease of use, and flexible detection of threats within individual enterprises and the correlation and sharing of those insights with their broader Collective Defense communities. Individual enterprises can choose to deploy our products and solutions using a variety of public and private cloud deployment options including AWS and Microsoft Azure. Enterprises that prefer to leverage their own private cloud infrastructure using hyper converged infrastructure can deploy our products and solutions through our partnership with Nutanix.

Flexible architecture for all enterprise networks

Our Collective Defense platform enables enterprises to add behavioral detection and Collective Defense to their on-premise, cloud, or multi-cloud infrastructure. Our platform can monitor workloads in major public cloud providers and on-premise physical and virtual networks from a single platform. Our Collective Defense platform can monitor network traffic and raw traffic in AWS and Azure or leverage existing logs to detect threats targeting their cloud infrastructure. With us, enterprises can apply the power of IronNet Collective Defense to their IT infrastructure and share collective threat intelligence with their Collective Defense community to detect threats targeting their community.

APIs / integrations

The Collective Defense platform and architecture is built around a rich set of APIs intended to efficiently and effectively complement and expand a customer's existing security infrastructure, such as SIEMs, EDRs, NGFWs, ITSM workflow tools, and other common cybersecurity tools. The platform includes the ability to query and interact with these tools, allowing customers and partners to integrate its detection into their security operations and to execute native response against detected threats. By connecting existing security systems to the IronNet Collective Defense platform, we allow our customers to drive higher efficiencies and value from their security investments. For example, we integrate with CrowdStrike to provide 1-click containment and can leverage CrowdStrike information to provide host details in the IronDefense Threat Hunting interface to deliver a seamless security operations experience across network and devices.

Data center operations

The Collective Defense platform utilizes a combination of global and customer infrastructure to deliver the solution. Customers can choose a variety of deployment options for their own enterprise however global and Collective Defense community level information is hosted in AWS data centers located in the United States and regional AWS data centers to support our international business. Our technology infrastructure, combined with the use of AWS resources, provides us with a distributed and scalable architecture on a global scale.

Our Services

Cyber Operations Center ("CyOC")

IronDefense customers can extend their SOC with our dedicated CyOC team, which comprises expert offensive and defensive cybersecurity operators with experience defending both private and public sectors against sophisticated threats. From monitoring to threat hunting, we enhance IronDefense capabilities by providing customers 24/7/365 NDR services backed by Collective Defense, enabling customer SOC analysts to spend more time focusing on strategic tasks.

Our cybersecurity operators add to the power of IronDefense by leveraging best practices to deliver advanced NDR capabilities that meet compliance standards. Our services are scalable, measurable, and cost- effective, and they provide complete real-time visibility into the network.

CyOC services include the following:

Hunt collaboration

Our Hunt Team comprises highly technical security analysts with real-world operational experience in defending highly secure networks across industries and sectors. Our analysts leverage our IronDefense platform to work side-by-side with customers' security operations personnel to detect and mitigate threats identified in the customer network.

Threat notifications

The CyOC team continually monitors and researches events and anomalies found in customer networks. The IronNet Customer Portal is used to notify customers of IronDefense findings of interest related to a customer's network. Notification is distributed to members determined by the customer and includes full event analysis and mitigation recommendation.

Rule deployment

The CyOC's Threat Intelligence analysts support customer operations by providing context to manual hunt operations and alert triage. The team produces tailored threat information to customer instances of IronDefense through Threat Intelligence Rule updates based on current suspicious and malicious IoCs, IronDome insights, emerging threat research, and results of research by our malware reverse engineers.

Reachback support

The CyOC team offers remote event collaboration, incident response, cybersecurity expertise, and platform support for IronDefense related security operations.

Reporting

Periodic insight reports are provided to customers on threat trends correlated to the customer's network and sector. These reports provide summarized and actionable IoCs associated with high risk network behaviors mapped to the MITRE ATT&CK Detection framework to identify the stage and progression of the threat. These reports also include a detailed list of resulting Threat Intelligence Rules deployed to customer instances of IronDefense.

Custom hunt tracking

Introductory and advanced training for end-users on analytics, alerts, entity enrichment, hunting, and network defense techniques are available. Periodic on-site side-by-side hunt operations, threat identification techniques, and review of newly implemented product features are also available.

Customer Success Team

Through our core products and services, we seek to increase our customers' visibility into the threat landscape, reduce the impact of a potential attack and improve the overall effectiveness of cybersecurity investments. One of the ways we do this is with our dedicated Customer Success ("**CS**") team. While some vendors charge a premium for expert Customer Success care, we include access to our CS team as part of a customer's subscription, including a dedicated Customer Success Manager for the life of the subscription.

At the onset of a new deployment, our CS team works with customer stakeholders to map out what success looks like, determine the key deliverables required to achieve those goals and create a success plan for the life of the partnership.

Governance and Maturity Services

These services measure adherence to specific regulatory or contractual requirements and provide measurable data as to the maturity of the organization's cybersecurity capabilities.

Cybersecurity Readiness Services

Given that threat actors continuously change their tactics, techniques, and procedures ("**TTP**"), these services are designed to ensure organizations are prepared for the latest and most immediate threats.

Incident Response Services

We provide incident response and digital forensic investigative services powered by an accomplished team with deep expertise. We specialize in providing incident response and digital forensic investigative services to companies of all sizes, ranging from large U.S. Fortune 50 companies to smaller organizations.

Training

Leveraging decades of cybersecurity experience, our results-focused training programs enable customers to unlock a higher level of cyber resilience. We adopt a hands-on approach to build technical proficiency and operational confidence using industry best practices. Cyber skillset training techniques include hunt methodology, offensive methodology, data analytics for security intelligence, SOC leadership, cyber threat intelligence operations, executive education, and custom cyber threat seminars.

Our Customers

Some of the world's largest enterprises, government organizations, high-profile brands, and governments trust us to protect their networks. The following graphic depicts our representative customers.

Customer case studies

Critical infrastructure customer case study: Southern Company

Within our first months in business, we had five major utility companies sharing cyber events in the IronDome across 25 states, helping secure infrastructure that delivers power to nearly 35 million customers.

Situation: Serving nine million customers across six states, Southern Company faced risks as a target for cyber attackers to steal information or disrupt operations.

Solution: As an early adopter of Collective Defense, one of the reasons Southern Company works with us is to get high quality, automated situational awareness and to move away from relying on manual methods.

Southern Company invested in its partnership with us to increase its ability to detect Advanced Persistent Threats, reduce dwell time and more quickly recover in the event of an attack.

Our relationship with Southern Company extends beyond just a vendor/client relationship, as senior leadership from both companies appear together at numerous events and government briefings to discuss their positions on topics like nuclear energy and the security of the U.S. power grid.

Southern Company's Chief Information Security Officer notes that "Broad situational awareness within sectors and across sectors is something we believe in, and why we are doing work with IronNet and many other partners in energy and other critical sectors, both nationally and internationally."

Critical infrastructure case study: American Electric Power ("AEP")

Situation: With the nation's largest transmission system consisting of more than 40,000 miles of transmission lines and more extra-high-voltage transmission lines than all other companies combined in North America, AEP needed to ensure the security of its own operations—while recognizing its role in contributing to the security of the electrical grid overall. collaborative cyber defense to combat adversaries.

Solution: Collective Defense provides the high-fidelity threat sharing to make AEP's cyber intelligence truly actionable, to ensure the cyber security of its 5.5 million customers.

AEP's Chief Security Officer says that "AEP values the relationship and initiatives being led by Gen. Alexander and IronNet."

Financial services customer case study: NBH Bank

Situation: National Bank Holdings ("**NBH**") needed a way to detect unknown threats. Monitoring only known threats, or "signatures" such as compromised domain names, IP addresses, or file hashes, missed a huge swath of threats that evade traditional signature-based threat detection. NBH needed a tool that could alert the security team of advanced threats across the cyber kill chain, in real time, in turn empowering the team to take action before the threat could affect operations.

Solution: After evaluating other platforms, NBH chose IronDefense for its ability to successfully detect malicious behaviors for DNS Tunneling, Domain Generation Algorithm ("**DGA**"), and Periodic Beaconing HTTP. As part of an IronDome, NBH has strengthened its ability to take proactive action against emerging threats detected by machine learning and further qualified by anonymized knowledge-sharing in the Collective Defense ecosystem.

NBH selected us because of our precise analytics; proactive hunt team support; partnership with our Customer Success team; and the ability to crowdsource expertise across their peers through Collective Defense.

NBH's VP of Enterprise Technology has stated that it views our Collective Defense as the "next big thing in cyber."

Sovereign wealth fund customer case study

Situation: An Asia-Pacific-based sovereign wealth fund with a $300 billion portfolio needed better visibility of network threats across its portfolio companies. Prior to implementing Collective Defense, neither the sovereign wealth fund nor its portfolio companies had a viable method for correlating IoCs across multiple organizations. They also lacked the ability to detect malicious threat activity based on network behaviors.

Solution: The company chose a Collective Defense IronDome to reduce time to detection via threat sharing across its portfolio companies.

In one instance, our analytics detected a sinister BotNet intrusion attempt into the firm's perimeter. The detection allowed the firm to act fast and catch the BotNet on their firewall before it got inside their network—all within 24 hours of detection.

The fund's Chief Technology Officer said that "None of our other threat hunting tools sparked an alarm. This may suggest that we can turn off some of our other threat hunting tools and save some money by using IronNet. This is IronNet value at work."

In addition to becoming our customer, the sovereign wealth fund also later became an investor in our company.

Oil & gas customer case study

Situation: A Fortune 500 midstream natural gas and crude oil pipeline company sought to increase its detection capabilities and accelerate threat response. Other methods of information sharing proved challenging for driving real business value.

Solution: IronDome provides visibility across the sector and an instantaneous way to share anonymized threat information, allowing the company to identify unknown threats faster and react more quickly. Based on network behavior, our detection analytics help the company to maximize the value of its other cybersecurity investments by identifying potential misconfigurations or gaps to tighten overall security.

According to the company's leader of Security Operations, "IronNet is truly a partner and not just another vendor."

Our Sales and Marketing

Sales

We use a "to and through" sales strategy. By maintaining a direct sales force consisting of senior-level account executives with deep security and high-tech experience, we have been able to leverage extensive professional networks and build inroads to strategic accounts. Because of this and the caliber of our senior leadership team, we believe we have a differentiated ability to convene CEOs, Chief Information Security Officers (CISOs) and other leaders within an entire industry, such as energy company CEOs. This is what enables our cornerstone/community selling approach.

We have three sales teams in the United States: Public Sector, covering federal, state and local segments; Critical Infrastructure, covering energy, oil & gas, and related segments; and Enterprise, covering financial services, insurance, tech, and a variety of other sectors. We have direct sales staff in six countries, as well as a growing portfolio of channel, managed services and technology partners across the United States, Europe, Middle East and Africa ("**EMEA**") and Asia-Pacific regions to scale our ability to discover, qualify, and close business.

In addition, we have inside sales development teams to expand our selling capabilities. These teams focus on early qualification and development of opportunities that we either close directly or transition to the field sales teams (for named accounts). These inside teams' primary objective is filling Collective Defense communities with smaller companies.

Marketing

Our marketing organization employs high-tech multichannel digital and content marketing for lead generation, aggressive public relations, social media and thought leadership programs to drive awareness, and specialization in strategies such as employee advocacy and search engine optimization. We were recently the top organic search engine result for "Network Detection and Response" in a competitive market.

Our public relations and media program has resulted in regular coverage in business press, cybersecurity trade media and industry trade media.

Our event program is focused on exposure to audiences that are aligned to our sales strategy. We incorporate a combination of both large industry events like Black Hat with regional and sector-focused events that allow us to capture leads on new customers to build out Collective Defense communities. Immediately at the onset of the COVID-19 pandemic, we pivoted our in-person event plan and launched a program of more than 40 webinars over the past 12 months with industry thought leaders. We also regularly host customers on our webinars as a strategic way to create customer case studies from transcripts.

We focus on providing compelling content for both demand generation and awareness-building. Our monthly Threat Intelligence Briefs summarize the IOCs and detections our SOC has discovered in order to inform the efforts of other operations analysts in the cybersecurity space. Our threat researchers produce in-depth analysis on topics such as ransomware detection and unique technical observations about the SUNBURST attack and other topics, which have been featured in media outlets. This helps build credibility with the security analyst audience, a key influencer in the buying process.

Our Partnership Ecosystem

Our partner ecosystem consists of leading organizations that have been carefully selected to help it deliver the power of Collective Defense across a variety of dimensions.

Technology partners

When used together, our partner integrations leverage our collective threat intelligence to react in real time, as well as proactively combat threats across the entire network, and create workflows that mitigate compromised devices. Our integrations are designed to increase the efficiency of security teams with smarter, more effective workflows built through collective threat intelligence. To streamline the alert triage and incident response processes, IronDefense can integrate with a number of security products, including:

SIEM tools to retrieve logs, share detections, and retrieve analyst feedback;

SOAR tools to share detections, retrieve analyst feedback, and augment existing playbooks;

EDR platforms to ingest endpoint event and entity context and initiate response to malicious activity; and

NGFW products to dynamically block malicious activity and ingest logs for analysis.

Current and planned future integrations and APIs include:

Cloud

AWS

Azure

GCP

SIEM

Splunk

IBM QRadar

Microsoft Azure Sentinel

LogRhythm

SOAR

Cortex XSOAR (formerly Demisto)

Splunk Phantom

Swimlane

ITSM

ServiceNow

EDR

CrowdStrike

Carbon Black

Forescout

Tanium

NGFW

Palo Alto Networks

Checkpoint Software Technologies

Zscaler

Go To Market ("GTM") Partners

With our GTM partners, we seek to accelerate service growth and value for their customers through a mutually beneficial program.

Raytheon Technologies

This partnership delivers cybersecurity solutions that defend against advanced threats that leverage behavior-based network traffic analysis and collective defense. The Raytheon-IronNet partnership combines our Collective Defense Platform with Raytheon's Managed Security Operations Center ("**MSOC**"), Managed Detection and Response ("**MDR**") and Cyber Security Operations Center ("**CSOC**") capabilities. This partnership delivers new analytical solutions that strengthen enterprise protection, along with a customized onboarding to integrate and operate the platform.

Accenture

We and Accenture work together to help companies protect critical infrastructure by quickly deploying and updating a system of machine-speed, advanced threat analytics across IT and Operational Technology, which automatically filters out the noise of false positives with the insight provided by community sourced context. Accenture provides the expertise in scalable implementation when it orchestrates our collective defense platform, delivering actionable attack information in real-time for their customers to prevent impact to critical infrastructure.

MDR/MSSP partners

Chosen channel partners work with us to develop and deliver an end-to-end solution designed to detect and prevent damaging and difficult-to-detect cyberattacks that continue to plague organizations across public and private sectors. For example, Jacobs' partnership with us brings together unique capabilities, helping customers to navigate the complexities of the current threat landscape more easily. Jacobs provides a full spectrum of professional services including consulting, technical, scientific and project delivery for the government and private sector. The joint offering of Jacobs and our collective defense platform brings advancements in machine learning and AI, which provides innovative cyber defense detection to discover both known and unknown cyber threats, allowing a more thorough and effective approach to network security for their clients.

/s/ John M. McConnell Vadm. John M. McConnell (Ret.)	Director	September 22, 2021
/s/ André Pienaar André Pienaar	Director	September 22, 2021
/s/ Michael J. Rogers Michael J. Rogers	Director	September 22, 2021
/s/ Theodore E. Schlein Theodore E. Schlein	Director	September 22, 2021
/s/ Jan E. Tighe Vadm. Jan E. Tighe (Ret.)	Director	September 22, 2021